Deutscher Bundestag **Drucksache 16/7218**

16. Wahlperiode 16. 11. 2007

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zu dem Übereinkommen des Europarats vom 23. November 2001 über Computerkriminalität

A. Problem und Ziel

Der Europarat hat am 23. November 2001 das Übereinkommen über Computerkriminalität beschlossen, das durch die Bundesrepublik Deutschland ratifiziert werden soll. Das Übereinkommen zielt auf einen Mindeststandard bei den Strafvorschriften über bestimmte schwere Formen der Computerkriminalität ab. Darüber hinaus enthält es Vorgaben für das Strafverfahrensrecht, die internationale Zusammenarbeit und zur Rechtshilfe.

B. Lösung

Durch den vorliegenden Gesetzentwurf sollen die Voraussetzungen nach Artikel 59 Abs. 2 Satz 1 des Grundgesetzes für die Ratifizierung des Übereinkommens geschaffen werden. Neben diesem Vertragsgesetz bedarf es weiterer, hiervon getrennter Ausführungsgesetze (Einundvierzigstes Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 7. August 2007, BGBl. I S. 1786; Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, Drucksache 16/5846, und Entwurf eines Gesetzes zur Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie, Drucksache 16/3439).

C. Alternativen

Keine

D. Finanzielle Auswirkungen

1. Haushaltsausgaben ohne Vollzugsaufwand

Keine

2. Vollzugsaufwand

Dem innerstaatlichen Umsetzungsbedarf durch Änderungen und Ergänzungen des Straf- und Strafprozessrechts wird durch die gesonderten Ausführungsgesetze Rechnung getragen, in denen auch der damit einhergehende Vollzugsaufwand dargestellt wird.

E. Sonstige Kosten

Für die Wirtschaft entstehen durch das Vertragsgesetz und die Ausführungsgesetze zur Bekämpfung der Computerkriminalität und zur Bekämpfung der sexuellen Ausbeutung von Kindern bei normgemäßem Verhalten keine Kosten. Die durch den Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG zu erwartenden Kosten für die Wirtschaft werden in dem Gesetzentwurf gesondert dargestellt. Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere das Verbraucherpreisniveau, sind nicht zu erwarten.

F. Bürokratiekosten

Es werden keine Informationspflichten für Bürgerinnen und Bürger, die Wirtschaft und Verwaltung neu eingefügt, geändert oder aufgehoben.

Allerdings bringt die spätere Ratifikation des Übereinkommens in geringem Umfang Informationspflichten für die Bundesverwaltung mit sich. Nach Artikel 24 Abs. 7 und Artikel 27 Abs. 2 des Übereinkommens sind dem Generalsekretär des Europarats die dort bestimmten Mitteilungen zu machen. Die Mitteilungspflichten fallen grundsätzlich nur einmal an und sind mit einem verhältnismäßig geringen Aufwand verbunden. Die Kosten dafür können nicht quantifiziert werden.

BUNDESREPUBLIK DEUTSCHLAND
DIE BUNDESKANZLERIN

Berlin, 15. November 2007

An den
Präsidenten des
Deutschen Bundestages
Herrn Dr. Norbert Lammert
Platz der Republik 1
11011 Berlin

Sehr geehrter Herr Präsident,

hiermit übersende ich den von der Bundesregierung beschlossenen

Entwurf eines Gesetzes zu dem Übereinkommen des
Europarats vom 23. November 2001 über Computerkriminalität

mit Begründung und Vorblatt.

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium der Justiz.

Die Stellungnahme des Nationalen Normenkontrollrates gemäß § 6 Abs. 1 NKRG ist als Anlage 2 beigefügt.

Der Bundesrat hat in seiner 838. Sitzung am 9. November 2007 gemäß Artikel 76 Absatz 2 des Grundgesetzes beschlossen, gegen den Gesetzentwurf keine Einwendungen zu erheben.

Mit freundlichen Grüßen

Anlage 1

Entwurf

Gesetz zu dem Übereinkommen des Europarats vom 23. November 2001 über Computerkriminalität

Vom

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Dem in Budapest am 23. November 2001 von der Bundesrepublik Deutschland unterzeichneten Übereinkommen des Europarats über Computerkriminalität wird zugestimmt. Das Übereinkommen wird nachstehend mit einer amtlichen deutschen Übersetzung veröffentlicht.

Artikel 2

(1) Dieses Gesetz tritt am Tage nach seiner Verkündung in Kraft.

(2) Der Tag, an dem das Übereinkommen nach seinem Artikel 36 Abs. 4 für die Bundesrepublik Deutschland in Kraft tritt, ist im Bundesgesetzblatt bekannt zu geben.

Begründung zum Vertragsgesetz

Zu Artikel 1

Auf das Übereinkommen findet Artikel 59 Abs. 2 Satz 1 des Grundgesetzes Anwendung, da es sich auf Gegenstände der Bundesgesetzgebung bezieht.

Zu Artikel 2

Die Bestimmung des Absatzes 1 entspricht dem Erfordernis des Artikels 82 Abs. 2 Satz 1 des Grundgesetzes.

Nach Absatz 2 ist der Zeitpunkt, zu dem das Übereinkommen nach seinem Artikel 36 Abs. 4 für die Bundesrepublik Deutschland in Kraft tritt, im Bundesgesetzblatt bekannt zu geben.

Schlussbemerkung

Das Vorhaben selbst wird Bund, Länder und Gemeinden nicht mit Mehrkosten belasten. Auswirkungen auf die Einzelpreise, das Preisniveau, insbesondere das Verbraucherpreisniveau, oder die Umwelt sind ebenfalls nicht zu erwarten. Dem innerstaatlichen Umsetzungsbedarf durch Änderungen und Ergänzungen des Straf- und Strafprozessrechts wird durch gesonderte Ausführungsgesetze Rechnung getragen, in denen auch der damit einhergehende Vollzugsaufwand dargestellt wird.

Die Ratifikation des Übereinkommens bringt in geringem Umfang Informationspflichten für die Bundesverwaltung mit sich:

Nach Artikel 24 Abs. 7 und Artikel 27 Abs. 2 des Übereinkommens sind dem Generalsekretär des Europarats die dort bestimmten Mitteilungen zu machen. Die Mitteilungspflichten fallen grundsätzlich nur einmal an und sind mit einem verhältnismäßig geringen Aufwand verbunden. Die Kosten dafür können nicht quantifiziert werden.

Übereinkommen über Computerkriminalität

Convention on Cybercrime

Convention sur la cybercriminalité

(Übersetzung)

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to

Préambule

Les Etats membres du Conseil de l'Europe et les autres Etats signataires,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres;

Reconnaissant l'intérêt d'intensifier la coopération avec les autres Etats parties à la Convention;

Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale;

Conscients des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques;

Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux;

Reconnaissant la nécessité d'une coopération entre les Etats et l'industrie privée dans la lutte contre la cybercriminalité,

Präambel

Die Mitgliedstaaten des Europarats und die anderen Staaten, die dieses Übereinkommen unterzeichnen –

in der Erwägung, dass es das Ziel des Europarats ist, eine engere Verbindung zwischen seinen Mitgliedern herbeizuführen;

in Anerkennung der Bedeutung einer verstärkten Zusammenarbeit mit den anderen Staaten, die Vertragsparteien dieses Übereinkommens sind;

überzeugt von der Notwendigkeit, vorrangig eine gemeinsame Strafrechtspolitik zu verfolgen, die den Schutz der Gesellschaft vor Computerkriminalität, unter anderem durch die Annahme geeigneter Rechtsvorschriften und die Förderung der internationalen Zusammenarbeit, zum Ziel hat;

eingedenk der tiefgreifenden Veränderungen, die durch die Digitalisierung, die Konvergenz und die kontinuierliche Globalisierung von Rechnernetzen hervorgerufen werden;

besorgt über die Gefahr, dass Rechnernetze und elektronische Informationen auch zur Begehung von Straftaten benutzt und Beweismaterial für Straftaten über solche Netze gespeichert und übermittelt werden können;

in der Erkenntnis, dass die Staaten und die Privatwirtschaft bei der Bekämpfung der Computerkriminalität zusammenarbei-

protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a

et le besoin de protéger les intérêts légitimes dans l'utilisation et le développement des technologies de l'information;

Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace;

Convaincus que la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable;

Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée;

Conscients également du droit à la protection des données personnelles, tel que spécifié, par exemple, par la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel;

Considérant la Convention des Nations Unies relative aux droits de l'enfant (1989) et la Convention de l'Organisation internationale du travail sur les pires formes de travail des enfants (1999);

Tenant compte des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, ainsi que d'autres traités similaires conclus entre les Etats membres du Conseil de l'Europe et d'autres Etats, et soulignant que la présente Convention a pour but de les compléter en vue de rendre plus efficaces les enquêtes et les procédures pénales portant sur des infractions pénales en relation avec des systèmes et des données informatiques, ainsi que de permettre la col-

ten und berechtigte Interessen am Einsatz und an der Entwicklung von Informationstechnologien geschützt werden müssen;

in der Überzeugung, dass zur wirksamen Bekämpfung der Computerkriminalität eine verstärkte, zügige und gut funktionierende internationale Zusammenarbeit in Strafsachen nötig ist;

in der Überzeugung, dass dieses Übereinkommen notwendig ist, um Handlungen gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computersystemen, Netzen und Computerdaten sowie den Missbrauch solcher Systeme, Netze und Daten zu verhüten, indem die Kriminalisierung des in diesem Übereinkommen beschriebenen Verhaltens und hinreichende Befugnisse zur wirksamen Bekämpfung dieser Straftaten vorgesehen werden, indem die Aufdeckung, Untersuchung und strafrechtliche Verfolgung solcher Straftaten sowohl auf nationaler als auch auf internationaler Ebene erleichtert werden und indem Vorkehrungen für eine rasche und zuverlässige internationale Zusammenarbeit getroffen werden;

eingedenk dessen, dass ein angemessenes Gleichgewicht gewahrt werden muss zwischen den Interessen der Strafverfolgung und der Achtung der grundlegenden Menschenrechte im Sinne der Konvention des Europarats von 1950 zum Schutz der Menschenrechte und Grundfreiheiten, des Internationalen Pakts der Vereinten Nationen von 1966 über bürgerliche und politische Rechte und anderer anwendbarer völkerrechtlicher Verträge auf dem Gebiet der Menschenrechte, in denen das Recht auf unbehinderte Meinungsfreiheit sowie das Recht auf freie Meinungsäußerung einschließlich des Rechts, ohne Rücksicht auf Staatsgrenzen Informationen und Ideen jeder Art sich zu beschaffen, zu empfangen und weiterzugeben, und das Recht auf Achtung des Privatlebens bekräftigt werden;

eingedenk auch des Rechts auf Schutz personenbezogener Daten, wie es zum Beispiel im Übereinkommen des Europarats von 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vorgesehen ist;

in Anbetracht des Übereinkommens der Vereinten Nationen von 1989 über die Rechte des Kindes sowie des Übereinkommens der Internationalen Arbeitsorganisation von 1999 über die schlimmsten Formen der Kinderarbeit;

unter Berücksichtigung der bestehenden Übereinkommen des Europarats über die Zusammenarbeit auf strafrechtlichem Gebiet sowie ähnlicher Verträge zwischen Mitgliedstaaten des Europarats und anderen Staaten und unter Hinweis darauf, dass diese Übereinkünfte durch das vorliegende Übereinkommen ergänzt werden sollen, damit die strafrechtlichen Ermittlungen und Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und -daten wirksamer werden und

criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

lecte des preuves électroniques d'une infraction pénale;

Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la criminalité dans le cyberespace, notamment des actions menées par les Nations Unies, l'OCDE, l'Union européenne et le G8;

Rappelant les Recommandations du Comité des Ministres nº R (85) 10 concernant l'application pratique de la Convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications, nº R (88) 2 sur des mesures visant à combattre la piraterie dans le domaine du droit d'auteur et des droits voisins, nº R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, nº R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, et nº R (89) 9 sur la criminalité en relation avec l'ordinateur, qui indique aux législateurs nationaux des principes directeurs pour définir certaines infractions informatiques, ainsi que nº R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information;

Eu égard à la Résolution nº 1, adoptée par les ministres européens de la Justice lors de leur 21e Conférence (Prague, 10 et 11 juin 1997), qui recommande au Comité des Ministres de soutenir les activités concernant la cybercriminalité menées par le Comité européen pour les problèmes criminels (CDPC) afin de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens d'investigation efficaces en matière d'infractions informatiques, ainsi qu'à la Résolution nº 3, adoptée lors de la 23e Conférence des ministres européens de la Justice (Londres, 8 et 9 juin 2000), qui encourage les parties aux négociations à poursuivre leurs efforts afin de trouver des solutions permettant au plus grand nombre d'Etats d'être parties à la Convention et qui reconnaît la nécessité de disposer d'un mécanisme rapide et efficace de coopération internationale qui tienne dûment compte des exigences spécifiques de la lutte contre la cybercriminalité;

Prenant également en compte le plan d'action adopté par les chefs d'Etat et de gouvernement du Conseil de l'Europe à l'occasion de leur 2e Sommet (Strasbourg, 10 et 11 octobre 1997) afin de trouver des réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe,

Sont convenus de ce qui suit:

Beweismaterial in elektronischer Form für eine Straftat erhoben werden kann;

erfreut über jüngste Entwicklungen, welche die internationale Verständigung und Zusammenarbeit bei der Bekämpfung der Computerkriminalität einschließlich der Maßnahmen der Vereinten Nationen, der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, der Europäischen Union und der G8-Staaten weiter fördern;

unter Hinweis auf die Empfehlungen des Ministerkomitees Nr. R (85) 10 über die praktische Anwendung des Europäischen Übereinkommens über die Rechtshilfe in Strafsachen in Bezug auf Rechtshilfeersuchen um Überwachung des Telekommunikationsverkehrs, Nr. R (88) 2 über die Piraterie im Bereich des Urheberrechts und verwandter Schutzrechte, Nr. R (87) 15 zur Regelung der Nutzung personenbezogener Daten im Polizeibereich, Nr. R (95) 4 über den Schutz personenbezogener Daten im Bereich der Telekommunikationsdienste unter besonderer Berücksichtigung von Telefondiensten sowie Nr. R (89) 9 über computerbezogene Straftaten, die Leitlinien für die nationalen Gesetzgeber betreffend die Definition bestimmter Computerstraftaten enthält, und Nr. R (95) 13 über strafprozessrechtliche Probleme in Zusammenhang mit der Informationstechnologie;

unter Hinweis auf die auf der 21. Konferenz der europäischen Justizminister (Prag, 10. und 11. Juni 1997) angenommene Entschließung Nr. 1, mit der dem Ministerkomitee empfohlen wurde, die Arbeit des Europäischen Ausschusses für Strafrechtsfragen (CDPC) auf dem Gebiet der Computerkriminalität zu unterstützen, um die innerstaatlichen Strafrechtsbestimmungen einander anzunähern und den Einsatz wirksamer Mittel zur Untersuchung solcher Straftaten zu ermöglichen, sowie im Hinblick auf die auf der 23. Konferenz der europäischen Justizminister (London, 8. und 9. Juni 2000) angenommene Entschließung Nr. 3, mit der die an den Verhandlungen beteiligten Parteien ermuntert wurden, sich weiter um geeignete Lösungen zu bemühen, damit möglichst viele Staaten Vertragsparteien des Übereinkommens werden können, und in der anerkannt wurde, dass ein schnelles und wirksames System der internationalen Zusammenarbeit nötig ist, das den besonderen Erfordernissen der Bekämpfung der Computerkriminalität gebührend Rechnung trägt;

ferner im Hinblick auf den Aktionsplan, den die Staats- und Regierungschefs des Europarats bei ihrer zweiten Gipfelkonferenz (Straßburg, 10. und 11. Oktober 1997) angenommen haben und mit dem auf der Grundlage der Standards und Werte des Europarats gemeinsame Antworten auf die Entwicklung der neuen Informationstechnologien gefunden werden sollen –

sind wie folgt übereingekommen:

Chapter I
Use of terms

Article 1
Definitions

For the purposes of this Convention:

a “computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c “service provider” means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;

d “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

Chapitre I
Terminologie

Article 1
Définitions

Aux fins de la présente Convention,

a l’expression «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d’un programme, un traitement automatisé de données;

b l’expression «données informatiques» désigne toute représentation de faits, d’informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu’un système informatique exécute une fonction;

c l’expression «fournisseur de services» désigne:

i toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d’un système informatique, et

ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

d «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu’élément de la chaîne de communication, indiquant l’origine, la destination, l’itinéraire, l’heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Kapitel I
Begriffsbestimmungen

Artikel 1
Begriffsbestimmungen

Im Sinne dieses Übereinkommens bedeutet

a) „Computersystem“ eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms automatische Datenverarbeitung durchführen;

b) „Computerdaten“ jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Computersystem geeigneten Form einschließlich eines Programms, das die Ausführung einer Funktion durch ein Computersystem auslösen kann;

c) „Diensteanbieter“

i) jede öffentliche oder private Stelle, die es Nutzern ihres Dienstes ermöglicht, mit Hilfe eines Computersystems zu kommunizieren;

ii) jede andere Stelle, die für einen solchen Kommunikationsdienst oder für seine Nutzer Computerdaten verarbeitet oder speichert;

d) „Verkehrsdaten“ alle Computerdaten in Zusammenhang mit einer Kommunikation unter Nutzung eines Computersystems, die von einem Computersystem, das Teil der Kommunikationskette war, erzeugt wurden und aus denen der Ursprung, das Ziel, der Leitweg, die Uhrzeit, das Datum, der Umfang oder die Dauer der Kommunikation oder die Art des für die Kommunikation benutzten Dienstes hervorgeht.

Chapter II
Measures to be taken at the national level

Section 1
Substantive criminal law

Title 1
Offences against the confidentiality, integrity and availability of computer data and systems

Article 2
Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its

Chapitre II
Mesures à prendre au niveau national

Section 1
Droit pénal matériel

Titre 1
Infractions contre la confidentialité, l’intégrité et la disponibilité des données et systèmes informatiques

Article 2
Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale,

Kapitel II
Innerstaatlich zu treffende Maßnahmen

Abschnitt 1
Materielles Strafrecht

Titel 1
Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen

Artikel 2
Rechtswidriger Zugang

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den unbefugten Zugang

domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

zu einem Computersystem als Ganzem oder zu einem Teil davon, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die Straftat unter Verletzung von Sicherheitsmaßnahmen, in der Absicht, Computerdaten zu erlangen, in anderer unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss.

Article 3

Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3

Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Artikel 3

Rechtswidriges Abfangen

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um das mit technischen Hilfsmitteln bewirkte unbefugte Abfangen nichtöffentlicher Computerdatenübermittlungen an ein Computersystem, aus einem Computersystem oder innerhalb eines Computersystems einschließlich elektromagnetischer Abstrahlungen aus einem Computersystem, das Träger solcher Computerdaten ist, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die Straftat in unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss.

Article 4

Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 4

Atteinte à l'intégrité des données

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Artikel 4

Eingriff in Daten

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um das unbefugte Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.

(2) Eine Vertragspartei kann sich das Recht vorbehalten, als Voraussetzung vorzusehen, dass das in Absatz 1 beschriebene Verhalten zu einem schweren Schaden geführt haben muss.

Article 5

System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 5

Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Artikel 5

Eingriff in ein System

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die unbefugte schwere Behinderung des Betriebs eines Computersystems durch Eingeben, Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.

Article 6

Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be ne-

Article 6

Abus de dispositifs

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent néces-

Artikel 6

Missbrauch von Vorrichtungen

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen

cessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a. i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

saires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:

i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;

ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,

dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et

b la possession d'un élément visé aux paragraphes a. i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a. ii du présent article.

Maßnahmen, um folgende Handlungen, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben:

a) das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen

i) einer Vorrichtung einschließlich eines Computerprogramms, die in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine nach den Artikeln 2 bis 5 umschriebene Straftat zu begehen;

ii) eines Computerpassworts, eines Zugangscodes oder ähnlicher Daten, die den Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon ermöglichen,

mit dem Vorsatz, sie zur Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat zu verwenden, und

b) den Besitz eines unter Buchstabe a Ziffer i oder ii bezeichneten Mittels mit dem Vorsatz, es zur Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat zu verwenden. Eine Vertragspartei kann als gesetzliche Voraussetzung vorsehen, dass die strafrechtliche Verantwortlichkeit erst mit Besitz einer bestimmten Anzahl dieser Mittel eintritt.

(2) Dieser Artikel darf nicht so ausgelegt werden, als begründe er die strafrechtliche Verantwortlichkeit in Fällen, in denen das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen oder der Besitz nach Absatz 1 nicht zum Zweck der Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat, sondern beispielsweise zum genehmigten Testen oder zum Schutz eines Computersystems erfolgt.

(3) Jede Vertragspartei kann sich das Recht vorbehalten, Absatz 1 nicht anzuwenden, sofern der Vorbehalt nicht das Verkaufen, Verbreiten oder anderweitige Verfügbarmachen der in Absatz 1 Buchstabe a Ziffer ii bezeichneten Mittel betrifft.

Title 2

Computer-related offences

Article 7

Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly

Titre 2

Infractions informatiques

Article 7

Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles

Titel 2

Computerbezogene Straftaten

Artikel 7

Computerbezogene Fälschung

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um folgende Handlungen, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben: das zu unechten Daten führende Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten in der Absicht, dass diese Daten für rechtliche Zwecke so angesehen oder ei-

readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8

Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data;

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3

Content-related offences

Article 9

Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

étaient authentiques, qu’elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8

Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:

a par toute introduction, altération, effacement ou suppression de données informatiques;

b par toute forme d’atteinte au fonctionnement d’un système informatique,

dans l’intention, frauduleuse ou délictueuse, d’obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Titre 3

Infractions se rapportant au contenu

Article 9

Infractions se rapportant à la pornographie enfantine

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu’ils sont commis intentionnellement et sans droit:

a la production de pornographie enfantine en vue de sa diffusion par le biais d’un système informatique;

b l’offre ou la mise à disposition de pornographie enfantine par le biais d’un système informatique;

c la diffusion ou la transmission de pornographie enfantine par le biais d’un système informatique;

d le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d’un système informatique;

e la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

2 Aux fins du paragraphe 1 ci-dessus, le terme «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle:

a un mineur se livrant à un comportement sexuellement explicite;

b une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;

ner Handlung zugrunde gelegt werden, als wären sie echt, gleichviel, ob die Daten unmittelbar lesbar und verständlich sind. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die strafrechtliche Verantwortlichkeit erst in Verbindung mit einer betrügerischen oder ähnlichen unredlichen Absicht eintritt.

Artikel 8

Computerbezogener Betrug

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um folgende Handlung, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben: die Beschädigung des Vermögens eines anderen durch

a) Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten;

b) Eingreifen in den Betrieb eines Computersystems

in der betrügerischen oder unredlichen Absicht, sich oder einem anderen unbefugt einen wirtschaftlichen Vorteil zu verschaffen.

Titel 3

Inhaltsbezogene Straftaten

Artikel 9

Straftaten mit Bezug zu Kinderpornographie

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um folgende Handlungen, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben:

a) das Herstellen von Kinderpornographie zum Zweck ihrer Verbreitung über ein Computersystem;

b) das Anbieten oder Verfügbarmachen von Kinderpornographie über ein Computersystem;

c) das Verbreiten oder Übermitteln von Kinderpornographie über ein Computersystem;

d) das Beschaffen von Kinderpornographie über ein Computersystem für sich selbst oder einen anderen;

e) den Besitz von Kinderpornographie in einem Computersystem oder auf einem Computerdatenträger.

(2) Im Sinne des Absatzes 1 umfasst der Ausdruck „Kinderpornographie“ pornographisches Material mit der visuellen Darstellung

a) einer minderjährigen Person bei eindeutig sexuellen Handlungen;

b) einer Person mit dem Erscheinungsbild einer minderjährigen Person bei eindeutig sexuellen Handlungen;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4

Offences related to infringements of copyright and related rights

Article 10

Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs

c des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

3 Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.

4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.

Titre 4

Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Article 10

Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

3 Une Partie peut, dans des circonstances bien délimitées, se réserver le

c) real erscheinender Bilder, die eine minderjährige Person bei eindeutig sexuellen Handlungen zeigen.

(3) Im Sinne des Absatzes 2 umfasst der Ausdruck „minderjährige Person" alle Personen, die das 18. Lebensjahr noch nicht vollendet haben. Eine Vertragspartei kann jedoch eine niedrigere Altersgrenze vorsehen, wobei 16 Jahre nicht unterschritten werden dürfen.

(4) Jede Vertragspartei kann sich das Recht vorbehalten, Absatz 1 Buchstaben d und e sowie Absatz 2 Buchstaben b und c ganz oder teilweise nicht anzuwenden.

Titel 4

Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte

Artikel 10

Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um Urheberrechtsverletzungen, wie sie im Recht dieser Vertragspartei aufgrund ihrer Verpflichtungen nach der Pariser Fassung der Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst vom 24. Juli 1971, dem Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums und dem WIPO-Urheberrechtsvertrag festgelegt sind, mit Ausnahme der nach diesen Übereinkünften verliehenen Urheberpersönlichkeitsrechte, wenn diese Handlungen vorsätzlich, in gewerbsmäßigem Umfang und mittels eines Computersystems begangen werden, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben.

(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um Verletzungen verwandter Schutzrechte, wie sie im Recht dieser Vertragspartei aufgrund ihrer Verpflichtungen nach dem Internationalen Abkommen über den Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendeunternehmen (Abkommen von Rom), dem Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums und dem WIPO-Vertrag über Darbietungen und Tonträger festgelegt sind, mit Ausnahme der nach diesen Übereinkünften verliehenen Urheberpersönlichkeitsrechte, wenn diese Handlungen vorsätzlich, in gewerbsmäßigem Umfang und mittels eines Computersystems begangen werden, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben.

(3) Eine Vertragspartei kann sich das Recht vorbehalten, eine strafrechtliche

1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.

Verantwortlichkeit nach den Absätzen 1 und 2 unter einer begrenzten Zahl von Umständen nicht vorzusehen, sofern andere wirksame Abhilfen zur Verfügung stehen und dieser Vorbehalt die internationalen Verpflichtungen dieser Vertragspartei aus den in den Absätzen 1 und 2 genannten völkerrechtlichen Übereinkünften nicht beeinträchtigt.

Title 5

Ancillary liability and sanctions

Article 11

Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12

Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the com-

Titre 5

Autres formes de responsabilité et de sanctions

Article 11

Tentative et complicité

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.

3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

Article 12

Responsabilité des personnes morales

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé:

a sur un pouvoir de représentation de la personne morale;

b sur une autorité pour prendre des décisions au nom de la personne morale;

c sur une autorité pour exercer un contrôle au sein de la personne morale.

2 Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne phy-

Titel 5

Weitere Formen der Verantwortlichkeit und Sanktionen

Artikel 11

Versuch und Beihilfe oder Anstiftung

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die vorsätzliche Beihilfe oder Anstiftung zur Begehung einer nach den Artikeln 2 bis 10 umschriebenen Straftat mit dem Vorsatz, dass eine solche Straftat begangen werde, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.

(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den Versuch der Begehung einer nach den Artikeln 3 bis 5 sowie 7, 8 und 9 Absatz 1 Buchstaben a und c umschriebenen Straftat, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.

(3) Jede Vertragspartei kann sich das Recht vorbehalten, Absatz 2 ganz oder teilweise nicht anzuwenden.

Artikel 12

Verantwortlichkeit juristischer Personen

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass juristische Personen für eine nach diesem Übereinkommen umschriebene Straftat verantwortlich gemacht werden können, die zu ihren Gunsten von einer natürlichen Person begangen wird, die entweder allein oder als Teil eines Organs der juristischen Person handelt und die eine Führungsposition innerhalb der juristischen Person innehat aufgrund

a) einer Vertretungsmacht für die juristische Person;

b) einer Befugnis, Entscheidungen im Namen der juristischen Person zu treffen;

c) einer Kontrollbefugnis innerhalb der juristischen Person.

(2) Neben den in Absatz 1 bereits vorgesehenen Fällen trifft jede Vertragspartei die erforderlichen Maßnahmen, um sicherzustellen, dass eine juristische Person verantwortlich gemacht werden kann, wenn mangelnde Überwachung oder Kontrolle durch eine in Absatz 1 genannte natürliche

mission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13

Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2

Procedural law

Title 1

Common provisions

Article 14

Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

sique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présente Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

3 Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.

4 Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

Article 13

Sanctions et mesures

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.

Section 2

Droit procédural

Titre 1

Dispositions communes

Article 14

Portée d'application des mesures du droit de procédure

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article:

a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention;

b à toutes les autres infractions pénales commises au moyen d'un système informatique; et

c à la collecte des preuves électroniques de toute infraction pénale.

Person die Begehung einer nach diesem Übereinkommen umschriebenen Straftat zugunsten der juristischen Person durch eine ihr unterstellte natürliche Person ermöglicht hat.

(3) Vorbehaltlich der Rechtsgrundsätze der Vertragspartei kann die Verantwortlichkeit einer juristischen Person straf-, zivil- oder verwaltungsrechtlicher Art sein.

(4) Diese Verantwortlichkeit berührt nicht die strafrechtliche Verantwortlichkeit der natürlichen Personen, welche die Straftat begangen haben.

Artikel 13

Sanktionen und Maßnahmen

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass die nach den Artikeln 2 bis 11 umschriebenen Straftaten mit wirksamen, verhältnismäßigen und abschreckenden Sanktionen, einschließlich Freiheitsentziehung, bedroht werden.

(2) Jede Vertragspartei stellt sicher, dass juristische Personen, die nach Artikel 12 verantwortlich gemacht werden, wirksamen, verhältnismäßigen und abschreckenden strafrechtlichen oder nichtstrafrechtlichen Sanktionen oder Maßnahmen, einschließlich Geldsanktionen, unterliegen.

Abschnitt 2

Verfahrensrecht

Titel 1

Allgemeine Bestimmungen

Artikel 14

Geltungsbereich verfahrensrechtlicher Bestimmungen

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die Befugnisse und Verfahren zu schaffen, die in diesem Abschnitt für die Zwecke spezifischer strafrechtlicher Ermittlungen oder Verfahren vorgesehen sind.

(2) Sofern in Artikel 21 nichts anderes vorgesehen ist, wendet jede Vertragspartei die in Absatz 1 bezeichneten Befugnisse und Verfahren an in Bezug auf

a) die nach den Artikeln 2 bis 11 umschriebenen Straftaten;

b) andere mittels eines Computersystems begangene Straftaten;

c) die Erhebung von in elektronischer Form vorhandenem Beweismaterial für eine Straftat.

3

a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15

Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature

3

a Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.

b Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services:

i qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et

ii qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé,

cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

Article 15

Conditions et sauvegardes

1 Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir

(3)

a) Jede Vertragspartei kann sich das Recht vorbehalten, die in Artikel 20 bezeichneten Maßnahmen nur auf Straftaten oder Kategorien von Straftaten anzuwenden, die in dem Vorbehalt bezeichnet sind; die Reihe dieser Straftaten oder Kategorien von Straftaten darf nicht enger gefasst sein als die Reihe der Straftaten, auf die sie die in Artikel 21 bezeichneten Maßnahmen anwendet. Jede Vertragspartei prüft die Möglichkeit, einen solchen Vorbehalt zu beschränken, damit die in Artikel 20 bezeichnete Maßnahme im weitesten Umfang angewendet werden kann.

b) Kann eine Vertragspartei aufgrund von Beschränkungen in ihren Rechtsvorschriften, die im Zeitpunkt der Annahme dieses Übereinkommens in Kraft sind, die in den Artikeln 20 und 21 bezeichneten Maßnahmen nicht auf Kommunikationen anwenden, die innerhalb eines Computersystems eines Diensteanbieters übermittelt werden, das

i) für eine geschlossene Nutzergruppe betrieben wird und

ii) sich keiner öffentlichen Kommunikationsnetze bedient und nicht mit einem anderen öffentlichen oder privaten Computersystem verbunden ist,

so kann diese Vertragspartei sich das Recht vorbehalten, diese Maßnahmen auf solche Kommunikationen nicht anzuwenden. Jede Vertragspartei prüft die Möglichkeit, einen solchen Vorbehalt zu beschränken, damit die in den Artikeln 20 und 21 bezeichneten Maßnahmen im weitesten Umfang angewendet werden können.

Artikel 15

Bedingungen und Garantien

(1) Jede Vertragspartei stellt sicher, dass für die Schaffung, Umsetzung und Anwendung der in diesem Abschnitt vorgesehenen Befugnisse und Verfahren Bedingungen und Garantien ihres innerstaatlichen Rechts gelten, die einen angemessenen Schutz der Menschenrechte und Freiheiten einschließlich der Rechte vorsehen, die sich aus ihren Verpflichtungen nach dem Übereinkommen des Europarats von 1950 zum Schutz der Menschenrechte und Grundfreiheiten, dem Internationalen Pakt der Vereinten Nationen von 1966 über bürgerliche und politische Rechte und anderen anwendbaren völkerrechtlichen Übereinkünften auf dem Gebiet der Menschenrechte ergeben und zu denen der Grundsatz der Verhältnismäßigkeit gehören muss.

(2) Diese Bedingungen und Garantien umfassen, soweit dies in Anbetracht der

of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2

Expedited preservation of stored computer data

Article 16

Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3 Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

Titre 2

Conservation rapide de données informatiques stockées

Article 16

Conservation rapide de données informatiques stockées

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2 Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Art der betreffenden Befugnis oder des betreffenden Verfahrens angebracht ist, unter anderem eine gerichtliche oder sonstige unabhängige Kontrolle, eine Begründung der Anwendung sowie die Begrenzung des Umfangs und der Dauer der Befugnis oder des Verfahrens.

(3) Soweit es mit dem öffentlichen Interesse, insbesondere mit einer geordneten Rechtspflege, vereinbar ist, berücksichtigt jede Vertragspartei die Auswirkungen der in diesem Abschnitt vorgesehenen Befugnisse und Verfahren auf die Rechte, Verantwortlichkeiten und berechtigten Interessen Dritter.

Titel 2

Umgehende Sicherung gespeicherter Computerdaten

Artikel 16

Umgehende Sicherung gespeicherter Computerdaten

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, damit ihre zuständigen Behörden die umgehende Sicherung bestimmter Computerdaten einschließlich Verkehrsdaten, die mittels eines Computersystems gespeichert wurden, anordnen oder in ähnlicher Weise bewirken können, insbesondere wenn Gründe zu der Annahme bestehen, dass bei diesen Computerdaten eine besondere Gefahr des Verlusts oder der Veränderung besteht.

(2) Führt eine Vertragspartei Absatz 1 so durch, dass eine Person im Wege einer Anordnung aufgefordert wird, bestimmte gespeicherte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden, sicherzustellen, so trifft diese Vertragspartei die erforderlichen gesetzgeberischen und anderen Maßnahmen, um diese Person zu verpflichten, die Unversehrtheit dieser Computerdaten so lange wie notwendig, längstens aber 90 Tage, zu sichern und zu erhalten, um den zuständigen Behörden zu ermöglichen, deren Weitergabe zu erwirken. Eine Vertragspartei kann vorsehen, dass diese Anordnung anschließend verlängert werden kann.

(3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den Verwahrer oder eine andere Person, welche die Computerdaten zu sichern hat, zu verpflichten, die Durchführung dieser Verfahren für den nach ihrem innerstaatlichen Recht vorgesehenen Zeitraum vertraulich zu behandeln.

(4) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

Article 17

Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3

Production order

Article 18

Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

Article 17

Conservation et divulgation partielle rapides de données relatives au trafic

1 Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires:

a pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; et

b pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Titre 3

Injonction de produire

Article 18

Injonction de produire

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:

a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et

b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

3 Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;

Artikel 17

Umgehende Sicherung und teilweise Weitergabe von Verkehrsdaten

(1) Jede Vertragspartei trifft in Bezug auf Verkehrsdaten, die nach Artikel 16 zu sichern sind, die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen,

a) dass die umgehende Sicherung von Verkehrsdaten unabhängig davon möglich ist, ob ein oder mehrere Diensteanbieter an der Übermittlung dieser Kommunikation beteiligt waren, und

b) dass Verkehrsdaten in einem solchen Umfang umgehend an die zuständige Behörde der Vertragspartei oder an eine von dieser Behörde bezeichnete Person weitergegeben werden, dass die Vertragspartei die Diensteanbieter und den Weg feststellen kann, auf dem die Kommunikation übermittelt wurde.

(2) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

Titel 3

Anordnung der Herausgabe

Artikel 18

Anordnung der Herausgabe

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen anzuordnen,

a) dass eine Person in ihrem Hoheitsgebiet bestimmte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden und die in einem Computersystem oder auf einem Computerdatenträger gespeichert sind, vorzulegen hat und

b) dass ein Diensteanbieter, der seine Dienste im Hoheitsgebiet der Vertragspartei anbietet, Bestandsdaten in Zusammenhang mit diesen Diensten, die sich in seinem Besitz oder unter seiner Kontrolle befinden, vorzulegen hat.

(2) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

(3) Im Sinne dieses Artikels bedeutet der Ausdruck „Bestandsdaten" alle in Form von Computerdaten oder in anderer Form enthaltenen Informationen, die bei einem Diensteanbieter über Teilnehmer seiner Dienste vorliegen, mit Ausnahme von Verkehrsdaten oder inhaltsbezogenen Daten, und durch die Folgendes festgestellt werden kann:

a) die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Maßnahmen und die Dauer des Dienstes;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4

Search and seizure of stored computer data

Article 19

Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;

c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Titre 4

Perquisition et saisie de données informatiques stockées

Article 19

Perquisition et saisie de données informatiques stockées

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire:

a à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et

b à un support du stockage informatique permettant de stocker des données informatiques

sur son territoire.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes:

a saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique;

b) die Identität des Teilnehmers, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen;

c) andere Informationen über den Ort, an dem sich die Kommunikationsanlage befindet, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen.

Titel 4

Durchsuchung und Beschlagnahme gespeicherter Computerdaten

Artikel 19

Durchsuchung und Beschlagnahme gespeicherter Computerdaten

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen,

a) ein Computersystem oder einen Teil davon sowie die darin gespeicherten Computerdaten und

b) einen Computerdatenträger, auf dem Computerdaten gespeichert sein können,

in ihrem Hoheitsgebiet zu durchsuchen oder in ähnlicher Weise darauf Zugriff zu nehmen.

(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass ihre Behörden, wenn sie ein bestimmtes Computersystem oder einen Teil davon nach Absatz 1 Buchstabe a durchsuchen oder in ähnlicher Weise darauf Zugriff nehmen und Grund zu der Annahme haben, dass die gesuchten Daten in einem anderen Computersystem oder einem Teil davon im Hoheitsgebiet der betreffenden Vertragspartei gespeichert sind, und diese Daten von dem ersten System aus rechtmäßig zugänglich oder verfügbar sind, die Durchsuchung oder den ähnlichen Zugriff rasch auf das andere System ausdehnen können.

(3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen, Computerdaten, auf die nach Absatz 1 oder 2 Zugriff genommen wurde, zu beschlagnahmen oder in ähnlicher Weise sicherzustellen. Diese Maßnahmen umfassen die Befugnis,

a) ein Computersystem oder einen Teil davon oder einen Computerdatenträger zu beschlagnahmen oder in ähnlicher Weise sicherzustellen;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5

Real-time collection of computer data

Article 20

Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred

b réaliser et conserver une copie de ces données informatiques;

c préserver l'intégrité des données informatiques stockées pertinentes;

d rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

4 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.

5 Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

Titre 5

Collecte en temps réel de données informatiques

Article 20

Collecte en temps réel des données relatives au trafic

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes:

a à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et

b à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes:

i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énon-

b) eine Kopie dieser Computerdaten anzufertigen und zurückzubehalten;

c) die Unversehrtheit der einschlägigen gespeicherten Computerdaten zu erhalten;

d) diese Computerdaten in dem Computersystem, auf das Zugriff genommen wurde, unzugänglich zu machen oder sie daraus zu entfernen.

(4) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen anzuordnen, dass jede Person, die Kenntnisse über die Funktionsweise des Computersystems oder über Maßnahmen zum Schutz der darin enthaltenen Daten hat, in vernünftigem Maß die notwendigen Auskünfte zu erteilen hat, um die Durchführung der in den Absätzen 1 und 2 genannten Maßnahmen zu ermöglichen.

(5) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

Titel 5

Erhebung von Computerdaten in Echtzeit

Artikel 20

Erhebung von Verkehrsdaten in Echtzeit

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen,

a) Verkehrsdaten, die mit bestimmten in ihrem Hoheitsgebiet mittels eines Computersystems übermittelten Kommunikationen in Zusammenhang stehen, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen und

b) einen Diensteanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu verpflichten,

i) solche Verkehrsdaten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder

ii) bei der Erhebung oder Aufzeichnung solcher Verkehrsdaten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen.

(2) Kann eine Vertragspartei die in Absatz 1 Buchstabe a bezeichneten Maßnahmen aufgrund der in ihrer innerstaatlichen

to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

cées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

Rechtsordnung festgelegten Grundsätze nicht treffen, so kann sie stattdessen die erforderlichen gesetzgeberischen und anderen Maßnahmen treffen, um sicherzustellen, dass Verkehrsdaten, die mit bestimmten in ihrem Hoheitsgebiet übermittelten Kommunikationen in Zusammenhang stehen, durch Anwendung technischer Mittel in diesem Hoheitsgebiet in Echtzeit erhoben oder aufgezeichnet werden.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

(3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um einen Diensteanbieter zu verpflichten, die Tatsache, dass eine nach diesem Artikel vorgesehene Befugnis ausgeübt wird, sowie alle Informationen darüber vertraulich zu behandeln.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

(4) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

Article 21

Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

Article 21

Interception de données relatives au contenu

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne:

a à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et

b à obliger un fournisseur de services, dans le cadre de ses capacités techniques:

i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

Artikel 21

Erhebung von Inhaltsdaten in Echtzeit

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden in Bezug auf eine Reihe schwerer Straftaten, die durch ihr innerstaatliches Recht zu bestimmen sind, zu ermächtigen,

a) inhaltsbezogene Daten bestimmter Kommunikationen in ihrem Hoheitsgebiet, die mittels eines Computersystems übermittelt wurden, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen und

b) einen Diensteanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu verpflichten,

i) solche inhaltsbezogenen Daten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder

ii) bei der Erhebung oder Aufzeichnung solcher inhaltsbezogener Daten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen.

(2) Kann eine Vertragspartei die in Absatz 1 Buchstabe a bezeichneten Maßnahmen aufgrund der in ihrer innerstaatlichen Rechtsordnung festgelegten Grundsätze nicht treffen, so kann sie stattdessen die erforderlichen gesetzgeberischen und anderen Maßnahmen treffen, um sicherzustellen, dass inhaltsbezogene Daten bestimmter Kommunikationen in ihrem Hoheitsgebiet durch Anwendung technischer Mittel in diesem Hoheitsgebiet in Echtzeit erhoben oder aufgezeichnet werden.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3

Jurisdiction

Article 22

Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Section 3

Compétence

Article 22

Compétence

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise:

a sur son territoire; ou

b à bord d'un navire battant pavillon de cette Partie; ou

c à bord d'un aéronef immatriculé selon les lois de cette Partie; ou

d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.

2 Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes.

3 Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5 Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites.

(3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um einen Diensteanbieter zu verpflichten, die Tatsache, dass eine nach diesem Artikel vorgesehene Befugnis ausgeübt wird, sowie alle Informationen darüber vertraulich zu behandeln.

(4) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

Abschnitt 3

Gerichtsbarkeit

Artikel 22

Gerichtsbarkeit

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre Gerichtsbarkeit über die nach den Artikeln 2 bis 11 umschriebenen Straftaten zu begründen, wenn die Straftat wie folgt begangen wird:

a) in ihrem Hoheitsgebiet;

b) an Bord eines Schiffes, das die Flagge dieser Vertragspartei führt;

c) an Bord eines Luftfahrzeugs, das nach dem Recht dieser Vertragspartei eingetragen ist, oder

d) von einem ihrer Staatsangehörigen, wenn die Straftat nach dem am Tatort geltenden Recht strafbar ist oder die Straftat außerhalb des Hoheitsbereichs irgendeines Staates begangen wird.

(2) Jede Vertragspartei kann sich das Recht vorbehalten, die in Absatz 1 Buchstaben b bis d oder in Teilen davon enthaltenen Vorschriften in Bezug auf die Gerichtsbarkeit nicht oder nur in bestimmten Fällen oder unter bestimmten Bedingungen anzuwenden.

(3) Jede Vertragspartei trifft die erforderlichen Maßnahmen, um ihre Gerichtsbarkeit über die in Artikel 24 Absatz 1 bezeichneten Straftaten in den Fällen zu begründen, in denen sich eine verdächtige Person in ihrem Hoheitsgebiet befindet und sie sie, nachdem ein Auslieferungsersuchen gestellt worden ist, nur deshalb nicht an eine andere Vertragspartei ausliefert, weil sie ihre Staatsangehörige ist.

(4) Dieses Übereinkommen schließt die Ausübung einer Strafgerichtsbarkeit durch eine Vertragspartei nach ihrem innerstaatlichen Recht nicht aus.

(5) Wird die Gerichtsbarkeit für eine mutmaßliche Straftat, die nach diesem Übereinkommen umschrieben ist, von mehr als einer Vertragspartei geltend gemacht, so konsultieren die beteiligten Vertragsparteien einander, soweit angebracht, um die für die Strafverfolgung geeignetste Gerichtsbarkeit zu bestimmen.

Chapter III

International co-operation

Section 1

General principles

Title 1

General principles relating to international co-operation

Article 23

General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2

Principles relating to extradition

Article 24

Extradition

1

a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

Chapitre III

Coopération internationale

Section 1

Principes généraux

Titre 1

Principes généraux relatifs à la coopération internationale

Article 23

Principes généraux relatifs à la coopération internationale

Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Titre 2

Principes relatifs à l'extradition

Article 24

Extradition

1

a Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.

b Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, la peine minimale prévue par ce traité ou cet arrangement s'applique.

2 Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à

Kapitel III

Internationale Zusammenarbeit

Abschnitt 1

Allgemeine Grundsätze

Titel 1

Allgemeine Grundsätze der internationalen Zusammenarbeit

Artikel 23

Allgemeine Grundsätze der internationalen Zusammenarbeit

Die Vertragsparteien arbeiten untereinander im Einklang mit diesem Kapitel im größtmöglichen Umfang zusammen, indem sie einschlägige völkerrechtliche Übereinkünfte über die internationale Zusammenarbeit in Strafsachen sowie Übereinkünfte, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurden, und innerstaatliche Rechtsvorschriften für Zwecke der Ermittlungen oder Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und -daten oder für die Erhebung von Beweismaterial in elektronischer Form für eine Straftat anwenden.

Titel 2

Grundsätze der Auslieferung

Artikel 24

Auslieferung

(1)

a) Dieser Artikel findet auf die Auslieferung zwischen den Vertragsparteien wegen der nach den Artikeln 2 bis 11 umschriebenen Straftaten Anwendung, sofern sie nach den Rechtsvorschriften der beiden beteiligten Vertragsparteien mit einer Freiheitsstrafe im Höchstmaß von mindestens einem Jahr oder mit einer schwereren Strafe bedroht sind.

b) Gilt nach einer Übereinkunft auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften oder nach einem Auslieferungsvertrag einschließlich des Europäischen Auslieferungsübereinkommens (SEV Nr. 24), der zwischen zwei oder mehr Vertragsparteien anwendbar ist, eine andere Mindeststrafe, so findet die nach dieser Übereinkunft oder nach diesem Vertrag vorgesehene Mindeststrafe Anwendung.

(2) Die in Absatz 1 beschriebenen Straftaten gelten als in jeden zwischen den Vertragsparteien bestehenden Auslieferungsvertrag einbezogene der Auslieferung unterliegende Straftaten. Die Vertragsparteien verpflichten sich, diese Straftaten als der Auslieferung unterliegende Straftaten in jeden zwischen ihnen zu schließenden

extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.

Auslieferungsvertrag aufzunehmen.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7

a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3

General principles relating to mutual assistance

Article 25

General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations

3 Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.

4 Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.

5 L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.

6 Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte, en temps utile, de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable, conformément à la législation de cette Partie.

7

a Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.

b Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.

Titre 3

Principes généraux relatifs à l'entraide

Article 25

Principes généraux relatifs à l'entraide

1 Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les in-

(3) Erhält eine Vertragspartei, welche die Auslieferung vom Bestehen eines Vertrags abhängig macht, ein Auslieferungsersuchen von einer anderen Vertragspartei, mit der sie keinen Auslieferungsvertrag hat, so kann sie dieses Übereinkommen als Rechtsgrundlage für die Auslieferung in Bezug auf die in Absatz 1 bezeichneten Straftaten ansehen.

(4) Vertragsparteien, welche die Auslieferung nicht vom Bestehen eines Vertrags abhängig machen, erkennen unter sich die in Absatz 1 bezeichneten Straftaten als der Auslieferung unterliegende Straftaten an.

(5) Die Auslieferung unterliegt den im Recht der ersuchten Vertragspartei oder in den geltenden Auslieferungsverträgen vorgesehenen Bedingungen einschließlich der Gründe, aus denen die ersuchte Vertragspartei die Auslieferung ablehnen kann.

(6) Wird die Auslieferung wegen einer in Absatz 1 bezeichneten Straftat allein aufgrund der Staatsangehörigkeit der verfolgten Person oder deswegen abgelehnt, weil die ersuchte Vertragspartei der Auffassung ist, sie habe die Gerichtsbarkeit über die Straftat, so unterbreitet die ersuchte Vertragspartei auf Ersuchen der ersuchenden Vertragspartei den Fall ihren zuständigen Behörden zum Zweck der Strafverfolgung und teilt der ersuchenden Vertragspartei zu gegebener Zeit das endgültige Ergebnis mit. Diese Behörden treffen ihre Entscheidung und betreiben ihre Ermittlungen und ihr Verfahren in derselben Weise wie bei jeder anderen vergleichbaren Straftat nach dem Recht dieser Vertragspartei.

(7)

a) Jede Vertragspartei teilt dem Generalsekretär des Europarats bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde die Bezeichnung und Anschrift jeder Behörde mit, die, falls kein Vertrag besteht, für die Stellung oder Entgegennahme eines Ersuchens um Auslieferung oder vorläufige Verhaftung zuständig ist.

b) Der Generalsekretär des Europarats erstellt und aktualisiert ein Verzeichnis der von den Vertragsparteien so bestimmten Behörden. Jede Vertragspartei stellt sicher, dass die in dem Verzeichnis enthaltenen Angaben stets richtig sind.

Titel 3

Allgemeine Grundsätze der Rechtshilfe

Artikel 25

Allgemeine Grundsätze der Rechtshilfe

(1) Die Vertragsparteien leisten einander im größtmöglichen Umfang Rechtshilfe für Zwecke der Ermittlungen oder

or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26

Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

fractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

2 Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.

3 Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

4 Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.

5 Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Article 26

Information spontanée

1 Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.

Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und -daten oder für die Erhebung von Beweismaterial in elektronischer Form für eine Straftat.

(2) Jede Vertragspartei trifft ferner die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den in den Artikeln 27 bis 35 bezeichneten Verpflichtungen nachzukommen.

(3) In dringenden Fällen kann jede Vertragspartei Rechtshilfeersuchen oder damit in Zusammenhang stehende Mitteilungen durch schnelle Kommunikationsmittel einschließlich Telefax oder elektronischer Post übersenden, soweit diese Mittel einen angemessenen Sicherheits- und Authentisierungsstandard bieten (erforderlichenfalls auch unter Einsatz einer Verschlüsselung) und eine förmliche Bestätigung folgt, wenn die ersuchte Vertragspartei dies verlangt. Die ersuchte Vertragspartei nimmt das Ersuchen entgegen und beantwortet es mit einem dieser schnellen Kommunikationsmittel.

(4) Soweit in den Artikeln dieses Kapitels nicht ausdrücklich etwas anderes vorgesehen ist, unterliegt die Rechtshilfe den im Recht der ersuchten Vertragspartei oder in den anwendbaren Rechtshilfeverträgen vorgesehenen Bedingungen einschließlich der Gründe, aus denen die ersuchte Vertragspartei die Zusammenarbeit ablehnen kann. Die ersuchte Vertragspartei darf das Recht auf Verweigerung der Rechtshilfe in Bezug auf die in den Artikeln 2 bis 11 bezeichneten Straftaten nicht allein mit der Begründung ausüben, dass das Ersuchen eine Straftat betrifft, die von ihr als fiskalische Straftat angesehen wird.

(5) Darf die ersuchte Vertragspartei nach diesem Kapitel die Rechtshilfe von der Bedingung abhängig machen, dass die beiderseitige Strafbarkeit gegeben ist, so gilt, gleichviel, ob die Straftat nach ihrem Recht in dieselbe Kategorie von Straftaten fällt oder mit dem gleichen Begriff benannt ist wie nach dem Recht der ersuchenden Vertragspartei, diese Bedingung als erfüllt, wenn die Handlung, die der Straftat, derentwegen um Rechtshilfe ersucht wird, zugrunde liegt, nach ihrem Recht eine Straftat darstellt.

Artikel 26

Unaufgeforderte Übermittlung von Informationen

(1) Eine Vertragspartei kann einer anderen Vertragspartei, soweit ihr innerstaatliches Recht es erlaubt und ohne vorheriges Ersuchen, Informationen übermitteln, die sie im Rahmen eigener Ermittlungen gewonnen hat, wenn sie der Auffassung ist, dass die Übermittlung dieser Informationen der anderen Vertragspartei bei der Einleitung oder Durchführung von Ermittlungen oder Verfahren wegen nach diesem Übereinkommen umschriebener Straftaten helfen oder dazu führen könnte, dass diese Vertragspartei ein Ersuchen um Zusammenarbeit nach diesem Kapitel stellt.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

2 Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

(2) Vor Übermittlung dieser Informationen kann die übermittelnde Vertragspartei um vertrauliche Behandlung oder um Verwendung nur unter bestimmten Bedingungen ersuchen. Kann die andere Vertragspartei diesem Ersuchen nicht entsprechen, so teilt sie dies der übermittelnden Vertragspartei mit; diese entscheidet dann, ob die Informationen dennoch übermittelt werden sollen. Nimmt die andere Vertragspartei die Informationen unter den vorgeschriebenen Bedingungen an, so ist sie an diese Bedingungen gebunden.

Title 4
Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27
Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2

a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by

Titre 4
Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

Article 27
Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

2

a Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution;

b Les autorités centrales communiquent directement les unes avec les autres;

c Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe;

d Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

3 Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie

Titel 4
Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte

Artikel 27
Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte

(1) Ist zwischen der ersuchenden und der ersuchten Vertragspartei ein Rechtshilfevertrag oder eine Übereinkunft, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurde, nicht in Kraft, so finden die Absätze 2 bis 9 Anwendung. Liegen ein solcher Vertrag, eine solche Übereinkunft oder solche Rechtsvorschriften vor, so findet dieser Artikel nur Anwendung, wenn die betreffenden Vertragsparteien übereinkommen, an Stelle des Vertrags, der Übereinkunft oder der Rechtsvorschriften die Absätze 2 bis 9 ganz oder teilweise anzuwenden.

(2)

a) Jede Vertragspartei bestimmt eine oder mehrere zentrale Behörden, welche die Aufgabe haben, Rechtshilfeersuchen abzusenden, zu beantworten, zu erledigen oder an die für die Erledigung zuständigen Behörden weiterzuleiten.

b) Die zentralen Behörden verkehren unmittelbar miteinander.

c) Jede Vertragspartei teilt dem Generalsekretär des Europarats bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde die Bezeichnung und Anschrift der nach diesem Absatz bestimmten Behörden mit.

d) Der Generalsekretär des Europarats erstellt und aktualisiert ein Verzeichnis der von den Vertragsparteien so bestimmten zentralen Behörden. Jede Vertragspartei stellt sicher, dass die in dem Verzeichnis enthaltenen Angaben stets richtig sind.

(3) Rechtshilfeersuchen nach diesem Artikel werden nach den von der ersuchenden Vertragspartei bezeichneten Ver-

the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9

a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Or-

requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.

4 Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise:

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

5 La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités.

6 Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement, ou sous réserve des conditions qu'elle juge nécessaires.

7 La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.

8 La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

9

a En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans un tel cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante.

b Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Orga-

fahren erledigt, sofern dies mit dem Recht der ersuchten Vertragspartei nicht unvereinbar ist.

(4) Zusätzlich zu den Ablehnungsgründen nach Artikel 25 Absatz 4 kann die ersuchte Vertragspartei die Rechtshilfe verweigern, wenn

a) das Ersuchen eine Straftat betrifft, die von der ersuchten Vertragspartei als politische oder als mit einer solchen zusammenhängende Straftat angesehen wird, oder

b) sie der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, ihre Souveränität, Sicherheit, öffentliche Ordnung (ordre public) oder andere wesentliche Interessen zu beeinträchtigen.

(5) Die ersuchte Vertragspartei kann die Durchführung der in einem Ersuchen genannten Maßnahmen aufschieben, wenn die Gefahr besteht, dass sie die von ihren Behörden geführten strafrechtlichen Ermittlungen oder Verfahren beeinträchtigen.

(6) Bevor die ersuchte Vertragspartei die Rechtshilfe verweigert oder aufschiebt, prüft sie, gegebenenfalls nach Konsultation der ersuchenden Vertragspartei, ob dem Ersuchen zum Teil oder vorbehaltlich der von ihr als erforderlich erachteten Bedingungen entsprochen werden kann.

(7) Die ersuchte Vertragspartei teilt der ersuchenden Vertragspartei umgehend das Ergebnis der Erledigung eines Rechtshilfeersuchens mit. Jede Ablehnung und jeder Aufschub des Ersuchens ist zu begründen. Die ersuchte Vertragspartei teilt der ersuchenden Vertragspartei gegebenenfalls auch die Gründe mit, aus denen die Erledigung des Ersuchens unmöglich ist oder sich wahrscheinlich erheblich verzögern wird.

(8) Die ersuchende Vertragspartei kann die ersuchte Vertragspartei bitten, das Vorliegen eines Ersuchens nach diesem Kapitel und dessen Inhalt vertraulich zu behandeln, soweit die Erledigung des Ersuchens nichts anderes gebietet. Kann die ersuchte Vertragspartei der erbetenen Vertraulichkeit nicht entsprechen, so teilt sie dies der ersuchenden Vertragspartei umgehend mit; diese entscheidet dann, ob das Ersuchen dennoch erledigt werden soll.

(9)

a) In dringenden Fällen können Rechtshilfeersuchen und damit in Zusammenhang stehende Mitteilungen unmittelbar von den Justizbehörden der ersuchenden Vertragspartei an die Justizbehörden der ersuchten Vertragspartei übermittelt werden. In diesen Fällen ist gleichzeitig über die zentrale Behörde der ersuchenden Vertragspartei eine Kopie an die zentrale Behörde der ersuchten Vertragspartei zu senden.

b) Jedes Ersuchen oder jede Mitteilung nach diesem Absatz kann über die Internationale Kriminalpolizeiliche Orga-

ganisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28

Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred

nisation internationale de police criminelle (Interpol).

c Lorsqu’une demande a été formulée en application de l’alinéa a. du présent article et lorsque l’autorité n’est pas compétente pour la traiter, elle la transmet à l’autorité nationale compétente et en informe directement la Partie requérante.

d Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.

e Chaque Partie peut informer le Secrétaire Général du Conseil de l’Europe, au moment de la signature ou du dépôt de son instrument de ratification, d’acceptation, d’approbation ou d’adhésion, que, pour des raisons d’efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

Article 28

Confidentialité et restriction d’utilisation

1 En l’absence de traité d’entraide ou d’arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s’appliquent. Elles ne s’appliquent pas lorsqu’un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d’appliquer à la place tout ou partie du présent article.

2 La Partie requise peut subordonner la communication d’informations ou de matériels en réponse à une demande:

a à la condition que ceux-ci restent confidentiels lorsque la demande d’entraide ne pourrait être respectée en l’absence de cette condition; ou

b à la condition qu’ils ne soient pas utilisés aux fins d’enquêtes ou de procédures autres que celles indiquées dans la demande.

3 Si la Partie requérante ne peut satisfaire à l’une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l’information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.

4 Toute Partie qui fournit des informations ou du matériel soumis à l’une des

nisation (Interpol) übermittelt werden.

c) Wird ein Ersuchen nach Buchstabe a übermittelt und ist die befasste Behörde für die Erledigung nicht zuständig, so leitet sie das Ersuchen an die zuständige Behörde ihres Landes weiter und setzt die ersuchende Vertragspartei unmittelbar davon in Kenntnis.

d) Ersuchen oder Mitteilungen nach diesem Absatz, die keine Zwangsmaßnahmen erfordern, können unmittelbar von den zuständigen Behörden der ersuchenden Vertragspartei den zuständigen Behörden der ersuchten Vertragspartei übermittelt werden.

e) Jede Vertragspartei kann dem Generalsekretär des Europarats bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde mitteilen, dass Ersuchen nach diesem Absatz aus Gründen der Effizienz an ihre zentrale Behörde zu richten sind.

Artikel 28

Vertraulichkeit und Beschränkung der Verwendung

(1) Ist zwischen der ersuchenden und der ersuchten Vertragspartei ein Rechtshilfevertrag oder eine Übereinkunft, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurde, nicht in Kraft, so findet dieser Artikel Anwendung. Liegen ein solcher Vertrag, eine solche Übereinkunft oder solche Rechtsvorschriften vor, so findet dieser Artikel nur Anwendung, wenn die betreffenden Vertragsparteien übereinkommen, an Stelle des Vertrags, der Übereinkunft oder der Rechtsvorschriften die Absätze 2 bis 4 ganz oder teilweise anzuwenden.

(2) Die ersuchte Vertragspartei kann die Überlassung von Informationen oder Unterlagen in Erledigung eines Ersuchens von der Bedingung abhängig machen, dass sie

a) vertraulich behandelt werden, wenn das Rechtshilfeersuchen ohne diese Bedingung nicht erledigt werden könnte, oder

b) nicht für andere als die in dem Ersuchen genannten Ermittlungen oder Verfahren verwendet werden.

(3) Kann die ersuchende Vertragspartei einer Bedingung nach Absatz 2 nicht entsprechen, so setzt sie die andere Vertragspartei umgehend davon in Kenntnis; diese entscheidet dann, ob die Informationen dennoch zur Verfügung gestellt werden sollen. Nimmt die ersuchende Vertragspartei die Bedingung an, so ist sie daran gebunden.

(4) Jede Vertragspartei, die Informationen oder Unterlagen unter einer in Ab-

to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.

satz 2 genannten Bedingung zur Verfügung stellt, kann von der anderen Vertragspartei verlangen, dass sie in Zusammenhang mit dieser Bedingung Angaben über die Verwendung der Informationen oder Unterlagen macht.

Section 2

Specific provisions

Title 1

Mutual assistance regarding provisional measures

Article 29

Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

Section 2

Dispositions spécifiques

Titre 1

Entraide en matière de mesures provisoires

Article 29

Conservation rapide de données informatiques stockées

1 Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

2 Une demande de conservation faite en application du paragraphe 1 doit préciser:

a l'autorité qui demande la conservation;

b l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent;

c les données informatiques stockées à conserver et la nature de leur lien avec l'infraction;

d toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique;

e la nécessité de la mesure de conservation; et

f le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

3 Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.

Abschnitt 2

Besondere Bestimmungen

Titel 1

Rechtshilfe bei vorläufigen Maßnahmen

Artikel 29

Umgehende Sicherung gespeicherter Computerdaten

(1) Eine Vertragspartei kann eine andere Vertragspartei um Anordnung oder anderweitige Bewirkung der umgehenden Sicherung von Daten ersuchen, die mittels eines Computersystems gespeichert sind, das sich im Hoheitsgebiet der anderen Vertragspartei befindet, und derentwegen die ersuchende Vertragspartei beabsichtigt, ein Rechtshilfeersuchen um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten zu stellen.

(2) Ein Ersuchen um Sicherung nach Absatz 1 hat Folgendes genau zu bezeichnen:

a) die Behörde, die um die Sicherung ersucht;

b) die Straftat, die Gegenstand der strafrechtlichen Ermittlungen oder Verfahren ist, und eine kurze Sachverhaltsdarstellung;

c) die gespeicherten Computerdaten, die zu sichern sind, und der Zusammenhang zwischen ihnen und der Straftat;

d) alle verfügbaren Informationen zur Ermittlung des Verwahrers der gespeicherten Computerdaten oder des Standorts des Computersystems;

e) die Notwendigkeit der Sicherung und

f) die Absicht der Vertragspartei, ein Rechtshilfeersuchen um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der gespeicherten Computerdaten zu stellen.

(3) Nach Eingang des von einer anderen Vertragspartei gestellten Ersuchens trifft die ersuchte Vertragspartei alle geeigneten Maßnahmen zur umgehenden Sicherung der bezeichneten Daten in Übereinstimmung mit ihrem innerstaatlichen Recht. Für die Zwecke der Erledigung eines Ersuchens wird die beiderseitige Strafbarkeit als Voraussetzung für die Vornahme dieser Sicherung nicht verlangt.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30

Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

4 Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.

5 En outre, une demande de conservation peut être refusée uniquement:

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

6 Lorsque la Partie requise estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de la Partie requérante, ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.

7 Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins soixante jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

Article 30

Divulgation rapide de données conservées

1 Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.

(4) Eine Vertragspartei, welche die beiderseitige Strafbarkeit als Voraussetzung für die Erledigung eines Rechtshilfeersuchens um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe gespeicherter Daten verlangt, kann sich in Bezug auf andere als die nach den Artikeln 2 bis 11 umschriebenen Straftaten das Recht vorbehalten, Ersuchen um Sicherung nach diesem Artikel abzulehnen, wenn sie Grund zu der Annahme hat, dass im Zeitpunkt der Weitergabe die Voraussetzung der beiderseitigen Strafbarkeit nicht erfüllt werden kann.

(5) Darüber hinaus kann ein Ersuchen um Sicherung nur abgelehnt werden, wenn

a) das Ersuchen eine Straftat betrifft, die von der ersuchten Vertragspartei als politische oder als mit einer solchen zusammenhängende Straftat angesehen wird, oder

b) die ersuchte Vertragspartei der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, ihre Souveränität, Sicherheit, öffentliche Ordnung (ordre public) oder andere wesentliche Interessen zu beeinträchtigen.

(6) Ist durch die Sicherung nach Ansicht der ersuchten Vertragspartei die künftige Verfügbarkeit der Daten nicht gewährleistet oder die Vertraulichkeit der Ermittlungen der ersuchenden Vertragspartei gefährdet oder in anderer Weise beeinträchtigt, so setzt sie die ersuchende Vertragspartei umgehend davon in Kenntnis; diese entscheidet dann, ob das Ersuchen dennoch erledigt werden soll.

(7) Jede Sicherung, die in Erledigung des in Absatz 1 bezeichneten Ersuchens vorgenommen wird, erfolgt für mindestens 60 Tage, damit die ersuchende Vertragspartei ein Ersuchen um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten stellen kann. Nach Eingang eines solchen Ersuchens werden die Daten weiterhin gesichert, bis über das Ersuchen entschieden worden ist.

Artikel 30

Umgehende Weitergabe gesicherter Verkehrsdaten

(1) Stellt die ersuchte Vertragspartei bei der Erledigung eines Ersuchens nach Artikel 29 um Sicherung von Verkehrsdaten bezüglich einer bestimmten Kommunikation fest, dass ein Diensteanbieter in einem anderen Staat an der Übermittlung dieser Kommunikation beteiligt war, so gibt die ersuchte Vertragspartei Verkehrsdaten in so ausreichender Menge an die ersuchende Vertragspartei umgehend weiter, dass dieser Diensteanbieter und der Weg, auf dem die Kommunikation übermittelt wurde, festgestellt werden können.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2

Mutual assistance regarding investigative powers

Article 31

Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32

Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary

2 La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement:

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

Titre 2

Entraide concernant les pouvoirs d'investigation

Article 31

Entraide concernant l'accès aux données stockées

1 Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.

2 La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre.

3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:

a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification; ou

b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

Article 32

Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie:

a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou

b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si

(2) Von der Weitergabe von Verkehrsdaten nach Absatz 1 darf nur abgesehen werden, wenn

a) das Ersuchen eine Straftat betrifft, die von der ersuchten Vertragspartei als politische oder als mit einer solchen zusammenhängende Straftat angesehen wird, oder

b) die ersuchte Vertragspartei der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, ihre Souveränität, Sicherheit, öffentliche Ordnung (ordre public) oder andere wesentliche Interessen zu beeinträchtigen.

Titel 2

Rechtshilfe in Bezug auf Ermittlungsbefugnisse

Artikel 31

Rechtshilfe beim Zugriff auf gespeicherte Computerdaten

(1) Eine Vertragspartei kann eine andere Vertragspartei um Durchsuchung oder ähnlichen Zugriff, um Beschlagnahme oder ähnliche Sicherstellung und um Weitergabe von Daten ersuchen, die mittels eines Computersystems gespeichert sind, das sich im Hoheitsgebiet der ersuchten Vertragspartei befindet, einschließlich Daten, die nach Artikel 29 gesichert worden sind.

(2) Die ersuchte Vertragspartei erledigt das Ersuchen, indem sie die in Artikel 23 bezeichneten völkerrechtlichen Übereinkünfte, sonstigen Übereinkünfte und Rechtsvorschriften anwendet und die anderen einschlägigen Bestimmungen dieses Kapitels einhält.

(3) Das Ersuchen ist umgehend zu erledigen, wenn

a) Gründe zu der Annahme bestehen, dass bei den einschlägigen Daten eine besondere Gefahr des Verlusts oder der Veränderung besteht oder

b) die in Absatz 2 bezeichneten Übereinkünfte und Rechtsvorschriften eine umgehende Zusammenarbeit vorsehen.

Artikel 32

Grenzüberschreitender Zugriff auf gespeicherte Computerdaten mit Zustimmung oder wenn diese öffentlich zugänglich sind

Eine Vertragspartei darf ohne die Genehmigung einer anderen Vertragspartei

a) auf öffentlich zugängliche gespeicherte Computerdaten (offene Quellen) zugreifen, gleichviel, wo sich die Daten geographisch befinden, oder

b) auf gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden, mittels eines Computersystems in ihrem Hoheitsge-

consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33

Mutual assistance in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34

Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3

24/7 Network

Article 35

24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2

a A Party's point of contact shall have the capacity to carry out communica-

la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Article 33

Entraide dans la collecte en temps réel de données relatives au trafic

1 Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.

2 Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

Article 34

Entraide en matière d'interception de données relatives au contenu

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Titre 3

Réseau 24/7

Article 35

Réseau 24/7

1 Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes:

a apport de conseils techniques;

b conservation des données, conformément aux articles 29 et 30;

c recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

2

a Le point de contact d'une Partie aura les moyens de correspondre avec le

biet zugreifen oder diese Daten empfangen, wenn sie die rechtmäßige und freiwillige Zustimmung der Person einholt, die rechtmäßig befugt ist, die Daten mittels dieses Computersystems an sie weiterzugeben.

Artikel 33

Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit

(1) Die Vertragsparteien leisten einander Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit in Zusammenhang mit bestimmten Kommunikationen in ihrem Hoheitsgebiet, die mittels eines Computersystems übermittelt werden. Vorbehaltlich des Absatzes 2 unterliegt die Rechtshilfe den nach innerstaatlichem Recht vorgesehenen Bedingungen und Verfahren.

(2) Jede Vertragspartei leistet zumindest in Bezug auf die Straftaten Rechtshilfe, bei denen die Erhebung von Verkehrsdaten in Echtzeit in einem gleichartigen inländischen Fall möglich wäre.

Artikel 34

Rechtshilfe bei der Erhebung von Inhaltsdaten in Echtzeit

Die Vertragsparteien leisten einander Rechtshilfe bei der Erhebung oder Aufzeichnung von Inhaltsdaten bestimmter Kommunikationen, die mittels eines Computersystems übermittelt werden, in Echtzeit, soweit dies nach ihren anwendbaren Verträgen und innerstaatlichen Rechtsvorschriften zulässig ist.

Titel 3

24/7-Netzwerk

Artikel 35

24/7-Netzwerk

(1) Jede Vertragspartei bestimmt eine Kontaktstelle, die an sieben Wochentagen 24 Stunden täglich zur Verfügung steht, um für Zwecke der Ermittlungen oder Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und -daten oder für die Erhebung von Beweismaterial in elektronischer Form für eine Straftat unverzüglich für Unterstützung zu sorgen. Diese Unterstützung umfasst die Erleichterung oder, sofern dies nach innerstaatlichem Recht und innerstaatlicher Praxis zulässig ist, die unmittelbare Durchführung folgender Maßnahmen:

a) fachliche Beratung;

b) Sicherung von Daten nach den Artikeln 29 und 30 und

c) Erheben von Beweismaterial, Erteilen von Rechtsauskünften und Ausfindigmachen verdächtiger Personen.

(2)

a) Die Kontaktstelle einer Vertragspartei muss über Möglichkeiten zur schnellen

tions with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV

Final provisions

Article 36

Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37

Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

point de contact d'une autre Partie selon une procédure accélérée.

b Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.

3 Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

Chapitre IV

Clauses finales

Article 36

Signature et entrée en vigueur

1 La présente Convention est ouverte à la signature des Etats membres du Conseil de l'Europe et des Etats non membres qui ont participé à son élaboration.

2 La présente Convention est soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.

3 La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats, incluant au moins trois Etats membres du Conseil de l'Europe, auront exprimé leur consentement à être liés par la Convention, conformément aux dispositions des paragraphes 1 et 2.

4 Pour tout Etat signataire qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de l'expression de son consentement à être lié par la Convention, conformément aux dispositions des paragraphes 1 et 2.

Article 37

Adhésion à la Convention

1 Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe peut, après avoir consulté les Etats contractants à la Convention et en avoir obtenu l'assentiment unanime, inviter tout Etat non membre du Conseil, n'ayant pas participé à son élaboration, à adhérer à la présente Convention. La décision est prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au Comité des Ministres.

Kommunikation mit der Kontaktstelle einer anderen Vertragspartei verfügen.

b) Ist die von einer Vertragspartei bestimmte Kontaktstelle nicht Teil der für die internationale Rechtshilfe oder Auslieferung zuständigen Behörde oder Behörden dieser Vertragspartei, so stellt die Kontaktstelle sicher, dass sie sich mit dieser Behörde oder diesen Behörden schnell abstimmen kann.

(3) Jede Vertragspartei stellt sicher, dass geschultes und entsprechend ausgestattetes Personal zur Verfügung steht, um die Arbeit des Netzwerks zu erleichtern.

Kapitel IV

Schlussbestimmungen

Artikel 36

Unterzeichnung und Inkrafttreten

(1) Dieses Übereinkommen liegt für die Mitgliedstaaten des Europarats und für Nichtmitgliedstaaten, die sich an der Ausarbeitung des Übereinkommens beteiligt haben, zur Unterzeichnung auf.

(2) Dieses Übereinkommen bedarf der Ratifikation, Annahme oder Genehmigung. Die Ratifikations-, Annahme- oder Genehmigungsurkunden werden beim Generalsekretär des Europarats hinterlegt.

(3) Dieses Übereinkommen tritt am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach dem Tag folgt, an dem fünf Staaten einschließlich mindestens drei Mitgliedstaaten des Europarats nach den Absätzen 1 und 2 ihre Zustimmung ausgedrückt haben, durch das Übereinkommen gebunden zu sein.

(4) Für jeden Unterzeichnerstaat, der später seine Zustimmung ausdrückt, durch das Übereinkommen gebunden zu sein, tritt es am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach dem Tag folgt, an dem er nach den Absätzen 1 und 2 seine Zustimmung ausgedrückt hat, durch das Übereinkommen gebunden zu sein.

Artikel 37

Beitritt zum Übereinkommen

(1) Nach Inkrafttreten dieses Übereinkommens kann das Ministerkomitee des Europarats nach Konsultation der Vertragsstaaten des Übereinkommens und mit deren einhelliger Zustimmung jeden Staat, der nicht Mitglied des Rates ist und der sich nicht an der Ausarbeitung des Übereinkommens beteiligt hat, einladen, dem Übereinkommen beizutreten. Der Beschluss wird mit der in Artikel 20 Buchstabe d der Satzung des Europarats vorgesehenen Mehrheit und mit einhelliger Zustimmung der Vertreter der Vertragsstaaten, die Anspruch auf einen Sitz im Ministerkomitee haben, gefasst.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

2 Pour tout Etat adhérent à la Convention, conformément au paragraphe 1 ci-dessus, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.

(2) Für jeden Staat, der dem Übereinkommen nach Absatz 1 beitritt, tritt es am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach Hinterlegung der Beitrittsurkunde beim Generalsekretär des Europarats folgt.

Article 38

Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 38

Application territoriale

1 Tout Etat peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera la présente Convention.

2 Tout Etat peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.

3 Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Artikel 38

Räumlicher Geltungsbereich

(1) Jeder Staat kann bei der Unterzeichnung oder bei der Hinterlegung seiner Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde einzelne oder mehrere Hoheitsgebiete bezeichnen, auf die dieses Übereinkommen Anwendung findet.

(2) Jeder Staat kann jederzeit danach durch eine an den Generalsekretär des Europarats gerichtete Erklärung die Anwendung dieses Übereinkommens auf jedes weitere in der Erklärung bezeichnete Hoheitsgebiet erstrecken. Das Übereinkommen tritt für dieses Hoheitsgebiet am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach Eingang der Erklärung beim Generalsekretär folgt.

(3) Jede nach den Absätzen 1 und 2 abgegebene Erklärung kann in Bezug auf jedes darin bezeichnete Hoheitsgebiet durch eine an den Generalsekretär des Europarats gerichtete Notifikation zurückgenommen werden. Die Rücknahme wird am ersten Tag des Monats wirksam, der auf einen Zeitabschnitt von drei Monaten nach Eingang der Notifikation beim Generalsekretär folgt.

Article 39

Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

- the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
- the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
- the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in re-

Article 39

Effets de la Convention

1 L'objet de la présente Convention est de compléter les traités ou les accords multilatéraux ou bilatéraux applicables existant entre les Parties, y compris les dispositions:

- de la Convention européenne d'extradition, ouverte à la signature le 13 décembre 1957, à Paris (STE nº 24);
- de la Convention européenne d'entraide judiciaire en matière pénale, ouverte à la signature le 20 avril 1959, à Strasbourg (STE nº 30);
- du Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale, ouvert à la signature le 17 mars 1978, à Strasbourg (STE nº 99).

2 Si deux ou plusieurs Parties ont déjà conclu un accord ou un traité relatif aux matières traitées par la présente Convention, ou si elles ont autrement établi leurs relations sur ces sujets, ou si elles le feront à l'avenir, elles ont aussi la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, au lieu de la présente Convention. Toutefois, lorsque

Artikel 39

Wirkungen des Übereinkommens

(1) Zweck dieses Übereinkommens ist es, die zwischen den Vertragsparteien bestehenden zwei- oder mehrseitigen Verträge oder Übereinkünfte zu ergänzen einschließlich

- des am 13. Dezember 1957 in Paris zur Unterzeichnung aufgelegten Europäischen Auslieferungsübereinkommens (SEV Nr. 24),
- des am 20. April 1959 in Straßburg zur Unterzeichnung aufgelegten Europäischen Übereinkommens über die Rechtshilfe in Strafsachen (SEV Nr. 30),
- des am 17. März 1978 in Straßburg zur Unterzeichnung aufgelegten Zusatzprotokolls zum Europäischen Übereinkommen über die Rechtshilfe in Strafsachen (SEV Nr. 99).

(2) Haben zwei oder mehr Vertragsparteien bereits eine Übereinkunft oder einen Vertrag über Fragen geschlossen, die in diesem Übereinkommen geregelt sind, oder haben sie ihre Beziehungen in diesen Fragen anderweitig geregelt oder sollten sie dies in Zukunft tun, so sind sie auch berechtigt, die Übereinkunft oder den Vertrag oder die entsprechenden Regelungen

spect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40

Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41

Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42

Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of

les Parties établiront leurs relations relatives aux matières faisant l'objet de la présente Convention d'une manière différente de celle y prévue, elles le feront d'une manière qui ne soit pas incompatible avec les objectifs et les principes de la Convention.

3 Rien dans la présente Convention n'affecte d'autres droits, restrictions, obligations et responsabilités d'une Partie.

Article 40

Déclarations

Par déclaration écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la faculté d'exiger, le cas échéant, un ou plusieurs éléments supplémentaires tels que prévus aux articles 2, 3, 6, paragraphe 1.b, 7, 9, paragraphe 3, et 27, paragraphe 9.e.

Article 41

Clause fédérale

1 Un Etat fédéral peut se réserver le droit d'honorer les obligations contenues dans le chapitre II de la présente Convention dans la mesure où celles-ci sont compatibles avec les principes fondamentaux qui gouvernent les relations entre son gouvernement central et les Etats constituants ou autres entités territoriales analogues, à condition qu'il soit en mesure de coopérer sur la base du chapitre III.

2 Lorsqu'il fait une réserve prévue au paragraphe 1, un Etat fédéral ne saurait faire usage des termes d'une telle réserve pour exclure ou diminuer de manière substantielle ses obligations en vertu du chapitre II. En tout état de cause, il se dote de moyens étendus et effectifs permettant la mise en œuvre des mesures prévues par ledit chapitre.

3 En ce qui concerne les dispositions de cette Convention dont l'application relève de la compétence législative de chacun des Etats constituants ou autres entités territoriales analogues, qui ne sont pas, en vertu du système constitutionnel de la fédération, tenus de prendre des mesures législatives, le gouvernement fédéral porte, avec son avis favorable, lesdites dispositions à la connaissance des autorités compétentes des Etats constituants, en les encourageant à adopter les mesures appropriées pour les mettre en œuvre.

Article 42

Réserves

Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratifi-

anzuwenden. Regeln Vertragsparteien ihre Beziehungen in den in diesem Übereinkommen geregelten Fragen jedoch anders als hierin vorgesehen, so tun sie dies in einer Weise, die zu den Zielen und Grundsätzen des Übereinkommens nicht in Widerspruch steht.

(3) Dieses Übereinkommen lässt andere Rechte, Beschränkungen, Pflichten und Verantwortlichkeiten einer Vertragspartei unberührt.

Artikel 40

Erklärungen

Jeder Staat kann durch eine an den Generalsekretär des Europarats gerichtete schriftliche Notifikation bei der Unterzeichnung oder bei der Hinterlegung seiner Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde erklären, dass er von der Möglichkeit Gebrauch macht, nach Artikel 2, Artikel 3, Artikel 6 Absatz 1 Buchstabe b, Artikel 7, Artikel 9 Absatz 3 und Artikel 27 Absatz 9 Buchstabe e zusätzliche Merkmale als Voraussetzung vorzusehen.

Artikel 41

Bundesstaatsklausel

(1) Ein Bundesstaat kann sich das Recht vorbehalten, Verpflichtungen nach Kapitel II so weit zu übernehmen, wie sie mit den Grundprinzipien vereinbar sind, welche die Beziehungen zwischen seiner Zentralregierung und seinen Gliedstaaten oder anderen gleichartigen Gebietseinheiten regeln, vorausgesetzt, er ist noch zur Zusammenarbeit nach Kapitel III in der Lage.

(2) Bringt ein Bundesstaat einen Vorbehalt nach Absatz 1 an, so darf er diesen Vorbehalt nicht anwenden, um seine Verpflichtungen nach Kapitel II auszuschließen oder wesentlich einzuschränken. Er sieht auf jeden Fall umfassende und wirksame Strafverfolgungsmöglichkeiten in Bezug auf Maßnahmen nach Kapitel II vor.

(3) Hinsichtlich derjenigen Bestimmungen dieses Übereinkommens, für deren Anwendung die Gliedstaaten oder anderen gleichartigen Gebietseinheiten die Gesetzgebungszuständigkeit besitzen, ohne nach der Verfassungsordnung des Bundes zum Erlass von Rechtsvorschriften verpflichtet zu sein, bringt die Bundesregierung den zuständigen Stellen dieser Staaten die genannten Bestimmungen befürwortend zur Kenntnis und ermutigt sie, geeignete Maßnahmen zu treffen, um sie durchzuführen.

Artikel 42

Vorbehalte

Jeder Staat kann durch eine an den Generalsekretär des Europarats gerichtete schriftliche Notifikation bei der Unterzeichnung oder bei der Hinterlegung seiner Ra-

ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

cation, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou les réserves prévues à l'article 4, paragraphe 2, à l'article 6, paragraphe 3, à l'article 9, paragraphe 4, à l'article 10, paragraphe 3, à l'article 11, paragraphe 3, à l'article 14, paragraphe 3, à l'article 22, paragraphe 2, à l'article 29, paragraphe 4, et à l'article 41, paragraphe 1. Aucune autre réserve ne peut être faite.

tifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde erklären, dass er von einem oder mehreren der in Artikel 4 Absatz 2, Artikel 6 Absatz 3, Artikel 9 Absatz 4, Artikel 10 Absatz 3, Artikel 11 Absatz 3, Artikel 14 Absatz 3, Artikel 22 Absatz 2, Artikel 29 Absatz 4 und Artikel 41 Absatz 1 vorgesehenen Vorbehalten Gebrauch macht. Weitere Vorbehalte sind nicht zulässig.

Article 43

Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 43

Statut et retrait des réserves

1 Une Partie qui a fait une réserve conformément à l'article 42 peut la retirer en totalité ou en partie par notification adressée au Secrétaire Général du Conseil de l'Europe. Ce retrait prend effet à la date de réception de ladite notification par le Secrétaire Général. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

2 Une Partie qui a fait une réserve comme celles mentionnées à l'article 42 retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent.

3 Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves comme celles mentionnées à l'article 42 des informations sur les perspectives de leur retrait.

Artikel 43

Status und Rücknahme von Vorbehalten

(1) Eine Vertragspartei, die einen Vorbehalt nach Artikel 42 angebracht hat, kann ihn durch eine an den Generalsekretär des Europarats gerichtete Notifikation ganz oder teilweise zurücknehmen. Die Rücknahme wird mit dem Eingang der Notifikation beim Generalsekretär wirksam. Wird in der Notifikation erklärt, dass die Rücknahme eines Vorbehalts zu einem in der Notifikation angegebenen Zeitpunkt wirksam werden soll, und liegt dieser Zeitpunkt später als der Zeitpunkt, an dem die Notifikation beim Generalsekretär eingeht, so wird die Rücknahme zu diesem späteren Zeitpunkt wirksam.

(2) Eine Vertragspartei, die einen Vorbehalt nach Artikel 42 angebracht hat, nimmt diesen Vorbehalt ganz oder teilweise zurück, sobald die Umstände dies erlauben.

(3) Der Generalsekretär des Europarats kann sich in regelmäßigen Abständen bei den Vertragsparteien, die einen oder mehrere Vorbehalte nach Artikel 42 angebracht haben, nach den Aussichten für eine Rücknahme dieses Vorbehalts oder dieser Vorbehalte erkundigen.

Article 44

Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall

Article 44

Amendements

1 Des amendements à la présente Convention peuvent être proposés par chaque Partie, et sont communiqués par le Secrétaire Général du Conseil de l'Europe aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer, conformément aux dispositions de l'article 37.

2 Tout amendement proposé par une Partie est communiqué au Comité européen pour les problèmes criminels (CDPC), qui soumet au Comité des Ministres son avis sur ledit amendement.

3 Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le CDPC et, après consultation avec les Etats non membres parties à la présente Convention, peut adopter l'amendement.

4 Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 du présent ar-

Artikel 44

Änderungen

(1) Jede Vertragspartei kann Änderungen dieses Übereinkommens vorschlagen; der Generalsekretär des Europarats übermittelt jeden Vorschlag den Mitgliedstaaten des Europarats, den Nichtmitgliedstaaten, die sich an der Ausarbeitung dieses Übereinkommens beteiligt haben, sowie jedem Staat, der nach Artikel 37 diesem Übereinkommen beigetreten oder zum Beitritt eingeladen worden ist.

(2) Jede von einer Vertragspartei vorgeschlagene Änderung wird dem Europäischen Ausschuss für Strafrechtsfragen (CDPC) übermittelt; dieser unterbreitet dem Ministerkomitee seine Stellungnahme zu dem Änderungsvorschlag.

(3) Das Ministerkomitee prüft den Änderungsvorschlag und die vom CDPC unterbreitete Stellungnahme und kann nach Konsultation der Nichtmitgliedstaaten, die Vertragsparteien des Übereinkommens sind, die Änderung annehmen.

(4) Der Wortlaut jeder vom Ministerkomitee nach Absatz 3 angenommenen Änderung wird den Vertragsparteien zur An-

be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45

Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46

Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Conven-

ticle est communiqué aux Parties pour acceptation.

5 Tout amendement adopté conformément au paragraphe 3 du présent article entre en vigueur le trentième jour après que toutes les Parties ont informé le Secrétaire Général de leur acceptation.

Article 45

Règlement des différends

1 Le Comité européen pour les problèmes criminels du Conseil de l'Europe (CDPC) est tenu informé de l'interprétation et de l'application de la présente Convention.

2 En cas de différend entre les Parties sur l'interprétation ou l'application de la présente Convention, les Parties s'efforceront de parvenir à un règlement du différend par la négociation ou par tout autre moyen pacifique de leur choix, y compris la soumission du différend au CDPC, à un tribunal arbitral qui prendra des décisions qui lieront les Parties au différend, ou à la Cour internationale de justice, selon un accord entre les Parties concernées.

Article 46

Concertation des Parties

1 Les Parties se concertent périodiquement, au besoin, afin de faciliter:

a l'usage et la mise en œuvre effectifs de la présente Convention, y compris l'identification de tout problème en la matière, ainsi que les effets de toute déclaration ou réserve faite conformément à la présente Convention;

b l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique;

c l'examen de l'éventualité de compléter ou d'amender la Convention.

2 Le Comité européen pour les problèmes criminels (CDPC) est tenu périodiquement au courant du résultat des concertations mentionnées au paragraphe 1.

3 Le CDPC facilite, au besoin, les concertations mentionnées au paragraphe 1 et adopte les mesures nécessaires pour aider les Parties dans leurs efforts visant à compléter ou amender la Convention. Au plus tard à l'issue d'un délai de trois ans à compter de l'entrée en vigueur de la présente Convention, le CDPC procédera, en coopération avec les Parties, à un réexamen de l'ensemble des dis-

nahme übermittelt.

(5) Jede nach Absatz 3 angenommene Änderung tritt am 30. Tag nach dem Tag in Kraft, an dem alle Vertragsparteien dem Generalsekretär mitgeteilt haben, dass sie sie angenommen haben.

Artikel 45

Beilegung von Streitigkeiten

(1) Der Europäische Ausschuss für Strafrechtsfragen (CDPC) wird über die Auslegung und Anwendung dieses Übereinkommens auf dem Laufenden gehalten.

(2) Im Fall einer Streitigkeit zwischen den Vertragsparteien über die Auslegung oder Anwendung dieses Übereinkommens bemühen sich die Vertragsparteien, die Streitigkeit durch Verhandlungen oder andere friedliche Mittel ihrer Wahl beizulegen, einschließlich der Befassung des CDPC, eines Schiedsgerichts, das für die Streitparteien bindende Entscheidungen fällt, oder des Internationalen Gerichtshofs, je nach Vereinbarung der betroffenen Vertragsparteien.

Artikel 46

Konsultationen der Vertragsparteien

(1) Die Vertragsparteien konsultieren einander bei Bedarf in regelmäßigen Abständen, um Folgendes zu erleichtern:

a) die wirksame Anwendung und Durchführung dieses Übereinkommens einschließlich des Erkennens dabei etwa auftretender Probleme sowie im Hinblick auf die Folgen von Erklärungen oder Vorbehalten, die nach diesem Übereinkommen abgegeben oder angebracht wurden;

b) den Informationsaustausch über wichtige rechtliche, politische und technologische Entwicklungen in Bezug auf die Computerkriminalität und die Erhebung von Beweismaterial in elektronischer Form;

c) Überlegungen über eine etwaige Ergänzung oder Änderung des Übereinkommens.

(2) Der Europäische Ausschuss für Strafrechtsfragen (CDPC) wird in regelmäßigen Abständen von dem Ergebnis der in Absatz 1 bezeichneten Konsultationen unterrichtet.

(3) Der CDPC fördert gegebenenfalls die in Absatz 1 bezeichneten Konsultationen und trifft die erforderlichen Maßnahmen, um die Vertragsparteien bei ihren Bemühungen um Ergänzung oder Änderung des Übereinkommens zu unterstützen. Spätestens drei Jahre nach Inkrafttreten dieses Übereinkommens führt der Europäische Ausschuss für Strafrechtsfragen (CDPC) in Zusammenarbeit mit den Ver-

tion's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47

Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48

Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

positions de la Convention et proposera, le cas échéant, les amendements appropriés.

4 Sauf lorsque le Conseil de l'Europe les prend en charge, les frais occasionnés par l'application des dispositions du paragraphe 1 sont supportés par les Parties, de la manière qu'elles déterminent.

5 Les Parties sont assistées par le Secrétariat du Conseil de l'Europe dans l'exercice de leurs fonctions découlant du présent article.

Article 47

Dénonciation

1 Toute Partie peut, à tout moment, dénoncer la présente Convention par notification au Secrétaire Général du Conseil de l'Europe.

2 La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

Article 48

Notification

Le Secrétaire Général du Conseil de l'Europe notifie aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer:

a toute signature;

b le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion;

c toute date d'entrée en vigueur de la présente Convention, conformément à ses articles 36 et 37;

d toute déclaration faite en application de l'article 40 ou toute réserve faite en application de l'article 42;

e tout autre acte, notification ou communication ayant trait à la présente Convention.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

Fait à Budapest, le 23 novembre 2001, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non membres qui ont participé à l'élaboration de la Convention et à tout Etat invité à y adhérer.

tragsparteien eine Überprüfung aller Bestimmungen des Übereinkommens durch und empfiehlt gegebenenfalls geeignete Änderungen.

(4) Kosten, die bei der Durchführung des Absatzes 1 entstehen, werden von den Vertragsparteien in der von ihnen zu bestimmenden Weise getragen, soweit sie nicht vom Europarat übernommen werden.

(5) Die Vertragsparteien werden bei der Wahrnehmung ihrer Aufgaben nach diesem Artikel vom Sekretariat des Europarats unterstützt.

Artikel 47

Kündigung

(1) Jede Vertragspartei kann dieses Übereinkommen jederzeit durch eine an den Generalsekretär des Europarats gerichtete Notifikation kündigen.

(2) Die Kündigung wird am ersten Tag des Monats wirksam, der auf einen Zeitabschnitt von drei Monaten nach Eingang der Notifikation beim Generalsekretär folgt.

Artikel 48

Notifikation

Der Generalsekretär des Europarats notifiziert den Mitgliedstaaten des Europarats, den Nichtmitgliedstaaten, die sich an der Ausarbeitung dieses Übereinkommens beteiligt haben, sowie jedem Staat, der diesem Übereinkommen beigetreten oder zum Beitritt eingeladen worden ist,

a) jede Unterzeichnung;

b) jede Hinterlegung einer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde;

c) jeden Zeitpunkt des Inkrafttretens dieses Übereinkommens nach den Artikeln 36 und 37;

d) jede Erklärung nach Artikel 40 und jeden Vorbehalt nach Artikel 42;

e) jede andere Handlung, Notifikation oder Mitteilung in Zusammenhang mit diesem Übereinkommen.

Zu Urkund dessen haben die hierzu gehörig befugten Unterzeichneten dieses Übereinkommen unterschrieben.

Geschehen zu Budapest am 23. November 2001 in englischer und französischer Sprache, wobei jeder Wortlaut gleichermaßen verbindlich ist, in einer Urschrift, die im Archiv des Europarats hinterlegt wird. Der Generalsekretär des Europarats übermittelt allen Mitgliedstaaten des Europarats, den Nichtmitgliedstaaten, die sich an der Ausarbeitung des Übereinkommens beteiligt haben, sowie allen zum Beitritt zu diesem Übereinkommen eingeladenen Staaten beglaubigte Abschriften.

Denkschrift

I. Allgemeines

Das Übereinkommen des Europarats vom 23. November 2001 über Computerkriminalität (ETS-Nr. 185) stellt die Bekämpfung der Computerkriminalität international auf eine neue rechtliche Grundlage. Ein Schwerpunkt des Übereinkommens ist die Schaffung eines strafrechtlichen Mindeststandards bei Angriffen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Computer- und Telekommunikationssystemen sowie ihrem Missbrauch zur Begehung von Straftaten. Außerdem enthält es Vorgaben zu strafprozessualen Maßnahmen zur Durchsuchung und Beschlagnahme von Beweismaterial bei derartigen Straftaten und Regelungen über die Verbesserung der internationalen Zusammenarbeit einschließlich der Rechtshilfe bei deren Verfolgung.

Das Übereinkommen wird durch das Zusatzprotokoll zum Übereinkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art (ETS-Nr. 189) ergänzt.

1. Entstehungsgeschichte

Vor dem Hintergrund der rasanten Entwicklung auf dem Gebiet der Informationstechnologie und des zunehmenden Missbrauchs von Computersystemen zur Begehung von Straftaten beschloss der Lenkungsausschuss für Strafrechtsfragen des Europarats (CDPC) im November 1996 die Einrichtung eines Sachverständigenausschusses für Computerkriminalität. Dieser Ausschuss erhielt auf der Sitzung des Komitees der Ministerbeauftragten vom 4. Februar 1997 die Bezeichnung „Committee of Experts on Crime in Cyberspace (PC-CY)“ – Sachverständigenausschuss für Computerkriminalität – und nahm seine Tätigkeit im April 1997 auf.

Das Mandat dieses Ausschusses bestand darin, bestimmte Fragestellungen im Lichte der Empfehlungen des Ministerkomitees Nr. R(89)9 über computerbezogene Straftaten und Nr. R(95)13 über strafverfahrensrechtliche Probleme im Zusammenhang mit der Informationstechnologie zu überprüfen und aufbauend auf dieser Überprüfung ein völkerrechtlich verbindliches Rechtsinstrument unter besonderer Berücksichtigung internationaler Aspekte vorzubereiten.

Insbesondere sollten folgende Themen erörtert werden:

- Straftaten im Cyberspace, vor allem solche, die unter Einsatz von Telekommunikationsnetzwerken begangen werden,
- andere Fragestellungen des materiellen Strafrechts, bei denen sich eine gemeinsame Basis zum Zwecke internationaler Zusammenarbeit anbieten könnte,
- der (auch grenzüberschreitende) Einsatz und die Anwendbarkeit von Zwangsmaßnahmen im technologischen Umfeld,
- die Frage der Zuständigkeit bei Straftaten im Datennetz und
- Fragestellungen der internationalen Zusammenarbeit bei der Ermittlung von Straftaten im Cyberspace.

An der Ausarbeitung des Übereinkommens waren Sachverständige aus 18 Mitgliedstaaten des Europarats (darunter auch Deutschland), zwei vom Sekretariat des Europarats bestellte wissenschaftliche Sachverständige und Vertreter der Europäischen Kommission und des Generalsekretariats des Rates der Europäischen Union sowie die Nichtmitgliedstaaten des Europarats Kanada, Japan, USA und Südafrika als Beobachter beteiligt. Die Verhandlungen des Übereinkommens konnten nach rund vier Jahren abgeschlossen werden, nachdem der CDPC das Mandat des PC-CY um ein Jahr bis zum 31. Dezember 2000 verlängert hatte.

Das Übereinkommen wurde vom Ministerkomitee des Europarats auf dessen 109. Sitzung am 8. November 2001 angenommen und am 23. November 2001 anlässlich der Internationalen Konferenz über Computerkriminalität in Budapest zur Zeichnung aufgelegt. Die Bundesrepublik Deutschland hat das Übereinkommen gemeinsam mit 25 anderen Mitgliedstaaten des Europarats und vier Nichtmitgliedstaaten (USA, Kanada, Japan, Südafrika) bereits bei der Auflegung gezeichnet.

Das Übereinkommen ist am 1. Juli 2004 international in Kraft getreten. Es wurde bislang von 43 Staaten gezeichnet und von 21 ratifiziert (Stand: 31. August 2007).

Im Anhang zu dieser Denkschrift findet sich ein (in die deutsche Sprache übersetzter) umfangreicher Erläuternder Bericht zum Übereinkommen, der ebenfalls vom Ministerkomitee angenommen wurde. Dieser Bericht ist zwar nicht verbindlich, stellt jedoch eine Auslegungshilfe von entscheidendem Gewicht dar.

2. Inhalt und Würdigung des Übereinkommens

Das aus 48 Artikeln bestehende Übereinkommen gliedert sich in vier Kapitel: I. Begriffsbestimmungen, II. Innerstaatlich zu treffende Maßnahmen, III. Internationale Zusammenarbeit und IV. Schlussbestimmungen. Kapitel II enthält dabei Abschnitte zum materiellen Strafrecht, zum Verfahrensrecht und zur Gerichtsbarkeit.

Das Übereinkommen enthält im Wesentlichen folgende Regelungen:

Begriffsbestimmungen:

- Artikel 1 enthält Definitionen wesentlicher Begriffe.

Innerstaatlich zu treffende Maßnahmen:

- Die Artikel 2 bis 6 enthalten Vorgaben zu Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen.
- Die Artikel 7 und 8 regeln computerbezogene Straftaten (computerbezogene Urkundenfälschung und -betrug).
- Artikel 9 enthält Vorgaben zu inhaltsbezogenen Straftaten mit Bezug zu Kinderpornographie.
- Artikel 10 regelt Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte.
- Die Artikel 11 bis 13 enthalten Vorschriften zu Versuch, Beteiligung, Verantwortlichkeit juristischer Personen sowie zu Sanktionen und Maßnahmen.

– Die Artikel 14 und 15 enthalten allgemeine verfahrensrechtliche Bestimmungen, Bedingungen und Garantien.
– Die Artikel 16 und 17 enthalten Regelungen zur umgehenden Sicherung gespeicherter Computerdaten.
– Die Artikel 18 und 19 regeln die Anordnung der Herausgabe, die Durchsuchung und Beschlagnahme gespeicherter Computerdaten.
– Die Artikel 20 und 21 enthalten Regelungen zur Erhebung von Verkehrs- und Inhaltsdaten in Echtzeit.
– Artikel 22 enthält Vorgaben zum internationalen Strafanwendungsrecht (Gerichtsbarkeit).

Internationale Zusammenarbeit:

– Die Artikel 23 bis 25 enthalten allgemeine Grundsätze der internationalen Zusammenarbeit sowie der Auslieferung und der Rechtshilfe.
– Artikel 26 regelt die unaufgeforderte Übermittlung von Informationen.
– Die Artikel 27 und 28 regeln das Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte.
– Die Artikel 29 und 30 enthalten besondere Bestimmungen über die Rechtshilfe bei der umgehenden Sicherung gespeicherter Computerdaten und Weitergabe gesicherter Verkehrsdaten.
– Artikel 31 regelt die Rechtshilfe beim Zugriff auf gespeicherte Computerdaten (Durchsuchung, Beschlagnahme).
– Artikel 32 enthält eine besondere Regelung zum grenzüberschreitenden Zugriff auf gespeicherte Computerdaten mit Zustimmung oder wenn diese öffentlich sind.
– Die Artikel 33 und 34 regeln die Rechtshilfe bei der Erhebung von Verkehrs- und Inhaltsdaten in Echtzeit.
– Artikel 35 enthält Regelungen zum 24/7-Netzwerk.

Schlussbestimmungen:

Die Artikel 36 bis 48 enthalten die üblichen Schlussbestimmungen zu völkerrechtlichen Verträgen (insbesondere Inkrafttreten, Beitritt, Vorbehalte, Erklärungen, Notifikation).

3. Deutsche Erklärung

Die Bundesregierung wird im Zuge der völkerrechtlichen Ratifikation des Übereinkommens die folgenden Erklärungen abgeben und Vorbehalte einlegen:

„In Übereinstimmung mit Artikel 40 des Übereinkommens wird erklärt, dass von der Möglichkeit Gebrauch gemacht wird,

a) nach Artikel 2 Satz 2 das zusätzliche Merkmal der Begehung der Straftat unter Verletzung von Sicherheitsmaßnahmen als Voraussetzung für die nach Artikel 2 Satz 1 im deutschen Recht umschriebene Straftat des Ausspähens von Daten in § 202a des Strafgesetzbuches und
b) nach Artikel 7 Satz 2 das zusätzliche Merkmal der „betrügerischen oder ähnlichen unredlichen Absicht" in Form der „Täuschung im Rechtsverkehr" als Voraussetzung für die nach Artikel 7 Satz 1 im deutschen Recht umschriebene Straftat der Fälschung beweiserheblicher Daten in § 269 des Strafgesetzbuches

vorzusehen."

Weiterhin erklärt die Bundesrepublik Deutschland, dass von Artikel 42 des Übereinkommens insoweit Gebrauch gemacht wird, als

a) Artikel 6 Abs. 1 Ziffer i im Hinblick auf das Tatmittel der „Vorrichtungen" und Buchstabe b nicht angewendet werden,
b) der Versuch der Begehung der nach Artikel 3 beschriebenen Handlungen nicht als Straftat nach dem innerstaatlichen Recht umschrieben werden und
c) für die Ersuchen um umgehende Sicherung von Daten nach Artikel 29 der Ablehnungsgrund der beiderseitigen Strafbarkeit gilt, es sei denn, es handelt sich um eine in den Artikeln 2 bis 11 umschriebene Straftat.

II. Besonderes

Im Einzelnen ist zu den Bestimmungen des Übereinkommens ergänzend zu dem als Anlage zur Denkschrift in deutscher Übersetzung wiedergegebenen Erläuternden Bericht Folgendes auszuführen:

Kapitel I
Begriffsbestimmungen

Zu Artikel 1 – Begriffsbestimmungen

In Artikel 1 werden vier im Übereinkommen verwendete Begriffe näher bestimmt. Der Erläuternde Bericht (Nummer 22) weist ausdrücklich darauf hin, dass diese Begriffe nicht wörtlich und in gleicher Form in innerstaatliches Recht umgesetzt werden müssen. Maßgeblich ist nur, dass das innerstaatliche Recht ein auf diese Begriffe aufbauendes, entsprechendes Schutzniveau bietet.

a) Computersystem

Im Sinne des Übereinkommens ist ein Computersystem eine aus Hard- und Software bestehende Vorrichtung, die zur automatischen Verarbeitung digitaler Daten entwickelt wurde. Der Begriff ist nicht so auszulegen, dass nunmehr auch Video-Geräte, CD-Player, Haushaltsgeräte und ähnliche Geräte umfasst wären, nur weil dort Chips oder elektronische Teile mit eingebaut sind. Bezüglich der Einzelheiten wird auf die Nummern 23 und 24 des Erläuternden Berichts verwiesen.

b) Computerdaten

Die hier verwendete Definition geht auf die entsprechende Definition der International Organization for Standardization (ISO) des Begriffs „Daten" zurück. Wesentliches Charakteristikum ist daher, dass Daten eine für die Verarbeitung in einem Computersystem geeignete Form aufweisen müssen.

Der Begriff der Daten in den Tatbeständen der Computerdelikte in den §§ 263a, 268 und 269 StGB sowie der engere Datenbegriff der §§ 202a bis 202c, 274, 303a, 303b StGB erfüllen diese Voraussetzungen ohne Weiteres, so dass Computerdaten und -programme erfasst sind.

c) Diensteanbieter

Dieser Begriff wird im Abschnitt zum Verfahrensrecht (Artikel 14, 17, 18, 20 und 21) und teilweise auch bei den Vorschriften über die Internationale Zusammenarbeit (Artikel 30) verwendet. Wesentliches Charakteristikum des Begriffs des Diensteanbieters ist, dass er seinen Nutzern ermöglicht, mit Hilfe eines Computersystems zu kommunizieren. Durch die Einbeziehung privater Organisationen in diesen Begriff ist sichergestellt, dass auch Dienste gegenüber geschlossenen Benutzergruppen wie beispielsweise im Rahmen eines unternehmensinternen Intranets erfasst werden. Neben öffentlichen und privaten Gruppen sind weiterhin auch solche Organisationen vom Begriff des Diensteanbieters erfasst, die für diese Gruppen oder deren Nutzer Daten speichern oder auf andere Weise verarbeiten. Damit scheiden reine „Inhaltsanbieter“ im Unterschied zu „Zugangsanbietern“ als Diensteanbieter aus.

d) Verkehrsdaten

Der Begriff der Verkehrsdaten findet sich im Abschnitt zum Verfahrensrecht (Artikel 16, 17 und 20) und zur Internationalen Zusammenarbeit (Artikel 30 und 33) wieder. Da Verkehrsdaten teilweise anderen Regelungen unterworfen sind als Computerdaten, werden sie gesondert definiert. Verkehrsdaten geben Auskunft über die näheren Umstände eines Kommunikationsvorgangs und sind insbesondere bei Ermittlungen wegen einer Straftat von Bedeutung, da sie die Quelle, das Ziel, den Standort und den Zeitpunkt der Kommunikation offenbaren. Dem nationalen Gesetzgeber bleibt überlassen, bei der Normierung von Eingriffsbefugnissen in Verkehrsdaten nach deren Vertraulichkeit zu differenzieren, wobei grundsätzlich davon auszugehen ist, dass die Eingriffsintensität geringer einzustufen ist als bei Inhaltsdaten. Die Grenze für nationale Eingriffsbefugnisse ist in Artikel 15 des Übereinkommens normiert.

Kapitel II
Innerstaatlich zu treffende Maßnahmen

Kapitel II gliedert sich in drei Abschnitte: Materielles Strafrecht (Artikel 2 bis 13); Verfahrensrecht (Artikel 14 bis 21) und Gerichtsbarkeit (Artikel 22).

Abschnitt 1 – Materielles Strafrecht

Die in Kapitel II Abschnitt 1 aufgezählten Straftaten dienen der Harmonisierung des materiellen Strafrechts und damit der Schaffung eines einheitlichen Mindeststandards, durch den die Bekämpfung der Computerkriminalität national wie auch international erleichtert werden soll.

Die in den Artikeln 2 bis 10 normierten Straftaten sind nach Schutzgütern geordnet jeweils einem eigenen Titel zugeordnet, aus dem sich bereits ihre Schutzrichtung ergibt. Im Wesentlichen müssen im Computerstrafrecht zwei große Gruppen unterschieden werden: Straftaten, die sich gegen die Vertraulichkeit, Integrität und Verfügbarkeit der Computerdaten oder -systeme richten (Artikel 2 bis 6), und Straftaten, bei denen unter Zuhilfenahme von Computersystemen andere Rechtsgüter angegriffen werden (Artikel 7 bis 10). Der Erläuternde Bericht weist ausdrücklich darauf hin, dass die Vertragsparteien geringfügige und unbedeutende Verstöße von der Anwendung der Artikel 2 bis 10 ausschließen können (vgl. Nummer 37).

Im Bereich des materiellen Strafrechts verwendet das Übereinkommen bei der Umschreibung der Tatbestände zumeist die Merkmale „unbefugt“ und „vorsätzlich“. In beiden Fällen ist die Umsetzung dieser Begriffe dem nationalen Recht überlassen worden. Aus deutscher Sicht bestehen in beiden Fällen keine Umsetzungsschwierigkeiten; insbesondere setzen sämtliche Computerstraftatbestände im deutschen Recht voraus, dass der Täter „unbefugt“ handelt (vgl. z. B. §§ 202a und 263a StGB), wobei mit dem Merkmal „unbefugt“ das allgemeine Merkmal der „Rechtswidrigkeit“ gemeint ist. Die Begriffe „unbefugt“ und „vorsätzlich“ sind von den allgemeinen Deliktsmerkmalen des Vorsatzes und der Rechtswidrigkeit im deutschen Recht vollständig abgedeckt.

Die Flexibilität der Vertragsstaaten bei der Umsetzung des Übereinkommens wird durch zahlreiche Einschränkungsmöglichkeiten erhöht, die gemäß Artikel 40 bei der Ratifikation in einer Erklärung festzuhalten sind. Außerdem besteht die Möglichkeit der Einlegung von Vorbehalten, wie aus Artikel 42 hervorgeht.

Zu Artikel 2 – Rechtswidriger Zugang

Nach dieser Vorgabe soll der „unbefugte Zugang“ zu einem Computersystem als Ganzes oder zu einem Teil unter Strafe gestellt werden. Erfasst werden hiermit vor allem diejenigen Handlungen, die als „Hacking“, also als das „Knacken“ eines Informationssystems, bezeichnet werden. „Unbefugt“ ist der Zugang unter anderem, wenn der Eigentümer oder Verfügungsberechtigte des Zugriffsobjekts hierin nicht eingewilligt hat. Auf einen „Teil“ eines Computersystems im Sinne der Vorschrift wird zugegriffen, wenn beispielsweise der Zugang zu Computerkomponenten wie Hard- und Software oder zu jeglicher Form von Daten verschafft wird.

Artikel 2 bedurfte der klarstellenden Umsetzung in das innerstaatliche Recht, da er von der bisherigen Fassung des § 202a StGB (Ausspähen von Daten), der auf das Verschaffen von Daten abstellte, nur zum Teil abgedeckt war. Zwar erfasste dieser Tatbestand faktisch schon vielfach das Hacking, da der Täter sich hierbei regelmäßig auch Daten verschafft. Aus Gründen der Klarstellung wurde durch das Einundvierzigste Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 7. August 2007 (BGBl. I S. 1786) eine Erweiterung des § 202a StGB dahingehend vorgenommen, dass bereits der bloße unbefugte Zugang zu besonders gesicherten Daten unter Überwindung von Sicherheitsmaßnahmen strafbar ist. Durch die Anknüpfung an den Datenbegriff ist auch der Zugriff auf nur einen Teil des Computersystems erfasst. Unbefugt ist der Zugang u. a. dann nicht, wenn eine (mutmaßliche) Einwilligung vorliegt. Zu den Einzelheiten wird auf die Begründung des Gesetzentwurfs für das Einundvierzigste Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) (BT-Drs. 16/3656) verwiesen.

Die Einschränkung des objektiven Tatbestandes auf besonders gesicherte Daten ist nach Artikel 2 Satz 2 möglich. Hiernach kann eine Vertragspartei u. a. als Voraussetzung vorsehen, dass die Straftat unter Verletzung von Sicherheitsmaßnahmen begangen worden sein muss.

Daher wird in Übereinstimmung mit Artikel 40 des Übereinkommens erklärt, dass von der Möglichkeit Gebrauch gemacht wird, nach Artikel 2 Satz 2 das zusätzliche Merkmal der Begehung der Straftat unter Verletzung von Sicherheitsmaßnahmen als Voraussetzung für die nach Artikel 2 Satz 1 im deutschen Recht umschriebene Straftat des Ausspähens von Daten in § 202a StGB vorzusehen.

Zu Artikel 3 – Rechtswidriges Abfangen

Artikel 3 enthält die Vorgabe, das unbefugte Abfangen nichtöffentlicher Computerdatenübermittlung an ein Computersystem, aus einem Computersystem oder innerhalb eines Computersystems einschließlich elektromagnetischer Abstrahlung aus einem Computersystem unter Strafe zu stellen.

Schutzgut dieser Vorschrift ist das Recht auf Nichtöffentlichkeit der Datenübermittlung. Die Vorschrift stellt sozusagen das Pendant zu dem „traditionellen“ Abhören und Aufzeichnen von Telefongesprächen dar und ist insoweit auch von der Schutzrichtung des Artikels 8 der Europäischen Menschenrechtskonvention (Recht auf Achtung der Korrespondenz) erfasst. Von Artikel 3 werden alle Formen der elektronischen Datenübertragung, wie beispielsweise E-Mail, Fax, Telefon, und „elektromagnetische Abstrahlungen“ aus Computersystemen erfasst. Abstrahlungen stellen zwar keine Daten im Sinne von Artikel 1 des Übereinkommens dar, können aber in solche umgewandelt werden und sind damit ebenso schutzwürdig.

Das geltende deutsche Strafrecht genügte den Anforderungen des Artikels 3 bisher nicht vollständig, da das unbefugte Abfangen von Daten nur fragmentarisch vom geltenden Recht erfasst wurde. So schützte § 202a StGB a. F. ausdrücklich zwar auch im Übermittlungsstadium befindliche Daten, aber nur dann, wenn sie besonders gesichert sind. Eine solche Einschränkung sieht jedoch Artikel 3 nicht vor.

Zur Umsetzung von Artikel 3 wurde daher durch das Einundvierzigste Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität ein gesonderter Tatbestand des Abfangens von Daten in einen neuen § 202b StGB eingefügt, der das unbefugte Sichverschaffen von Daten aus einer nichtöffentlichen Datenübermittlung und aus einer elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage unter Anwendung von technischen Mitteln erfasst, und zwar unabhängig davon, ob die Daten besonders gesichert sind oder nicht. Zu den Einzelheiten wird auf die Begründung des Gesetzentwurfs für das 41. StrÄndG (BT-Drs. 16/3656) verwiesen.

Von den weiteren Einschränkungsmöglichkeiten in Artikel 3 Satz 2 soll kein Gebrauch gemacht werden.

Zu Artikel 4 – Eingriff in Daten

Diese Vorschrift verleiht Computerdaten einen den körperlichen Gegenständen vergleichbaren Schutz im Hinblick auf deren vorsätzliche Beschädigung. Sie schützt die Integrität, die sachgemäße Funktionsweise und Anwendung gespeicherter Computerdaten und -programme. Tathandlung ist das vorsätzliche und unbefugte Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten. Nicht „unbefugt“ sein sollen unter anderem gängige Tätigkeiten, die in der Netzwerkgestaltung begründet sind oder gängige Betriebs- oder Unternehmenspraktiken (vgl. Nummer 62 des Erläuternden Berichts).

Artikel 4 ist durch § 303a StGB (Datenveränderung) vollständig umgesetzt, der das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten erfasst.

Unschädlich ist hierbei, dass die in Artikel 3 vorgesehenen Tathandlungen „Beschädigen“ und „Beeinträchtigen“ nicht ausdrücklich genannt werden, da der Schutzumfang des § 303a StGB umfassend konzipiert ist und solche Tathandlungen auch unter das Merkmal „verändern“ subsumiert werden können. Das Tatbestandsmerkmal „unbefugt“ braucht nicht eingefügt zu werden, da nach herrschender Meinung § 303a StGB ohnehin nur die unbefugte Datenerhebung erfasst.

Die Einlegung eines Vorbehalts nach Artikel 4 Abs. 2 des Übereinkommens ist nicht erforderlich.

Zu Artikel 5 – Eingriff in ein System

Artikel 5 erfasst die Fälle der Computersabotage. Schutzgut ist das Interesse der Betreiber und Benutzer von Computer- oder Telekommunikationsanlagen an deren ordnungsgemäßer Funktionsweise.

Tathandlung ist die unbefugte schwere Behinderung des Betriebs eines Computersystems durch Eingeben, Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten.

Artikel 5 wurde von § 303b StGB a. F. (Computersabotage) nur zum Teil erfasst. Umsetzungsbedarf bestand im Hinblick auf die Tathandlungen des „Eingebens“ und „Übertragens“ und insoweit, als § 303b StGB bisher nur Datenverarbeitungen von fremden Unternehmen und Behörden, nicht aber auch private Computersysteme erfasste.

Zur Umsetzung von Artikel 5 war daher eine Ergänzung des § 303b StGB erforderlich. Durch das Einundvierzigste Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität wurde der Anwendungsbereich des Absatzes 1 erweitert. Dieser wurde auf alle Datenverarbeitungen ausgedehnt, die „für einen anderen“ von wesentlicher Bedeutung sind. Außerdem wurden in einer neuen Nummer 2 die Tathandlungen des Eingebens und Übermittelns eingefügt.

Das Merkmal „von wesentlicher Bedeutung“ wurde aufrechterhalten. Es dient als Filter für Bagatellfälle, die durch den Tatbestand nicht erfasst werden sollen. Eine solche Einschränkung ist nach Artikel 5 des Europarat-Übereinkommens auch zulässig, der eine „schwere Behinderung“ verlangt. Da die Festlegung der Kriterien, ab denen eine Behinderung als „schwer“ und damit als strafwürdig anzusehen ist, den Vertragsstaaten überlassen ist (vgl. Nummer 67 des Erläuternden Berichts), kann für die Bestimmung auch an das Erfordernis der wesentlichen Bedeutung einer Datenverarbeitungsanlage angeknüpft werden, um unerhebliche Beeinträchtigungen auszuschließen. Zu den Einzelheiten wird auf die Begründung des Gesetzentwurfs für das 41. StrÄndG (BT-Drs. 16/3656) verwiesen.

Zu Artikel 6 – Missbrauch von Vorrichtungen

Artikel 6 enthält die Vorgabe, bestimmte Handlungen im Vorfeld der nach den Artikeln 2 bis 5 geregelten Computerstraftaten unter Strafe zu stellen.

Tatobjekt des Absatzes 1 Buchstabe a sind zum einen Vorrichtungen einschließlich Computerprogramme, die in erster Linie zu dem Zweck ausgelegt oder hergestellt worden sind, eine der nach den Artikeln 2 bis 5 festgelegten Straftaten zu begehen (i). Zum anderen sind es Computerpasswörter, Zugriffscodes oder ähnliche Daten, die den Zugriff auf ein Computersystem als Ganzes oder auf einen Teil davon ermöglichen (ii). Strafbar ist das Herstellen, Verkaufen, Beschaffen zwecks Gebrauch, Einführen, Verbreiten oder anderweitiges Zugänglichmachen.

Tathandlung nach Absatz 1 Buchstabe b ist der Besitz eines der in Absatz 1 Buchstabe a genannten Tatobjekte.

In subjektiver Hinsicht ist in den Fällen des Absatzes 1 Buchstabe a und b neben dem allgemeinen Tatvorsatz der Vorsatz erforderlich, eine der nach den Artikeln 2 bis 5 festgelegten Straftaten zu begehen.

Artikel 6 bedurfte der Umsetzung in innerstaatliches Recht. Ein Tatbestand, der Vorbereitungshandlungen zur Begehung von Computerstraftaten erfasst, existierte im deutschen Strafgesetzbuch bisher nur für den Computerbetrug (§ 263a Abs. 3 StGB), nicht aber für die Straftatbestände nach den Artikeln 2 bis 5 des Übereinkommens.

Das Einundvierzigste Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität sieht hierfür einen neuen Straftatbestand in § 202c StGB zur Umsetzung von Absatz 1 Buchstabe a Ziffer i und ii vor. Hiernach ist strafbar, wer eine Straftat nach § 202a oder § 202b StGB vorbereitet, indem er entweder Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht. § 202c StGB findet außerdem in den Fällen der Datenveränderung und der Computersabotage Anwendung (siehe §§ 303a, 303b StGB). Zu den Einzelheiten wird auf die Begründung des Umsetzungsgesetzes (BT-Drs. 16/3656) verwiesen.

Von der Vorbehaltsmöglichkeit in Absatz 3 soll hinsichtlich der Besitzstrafbarkeit in Absatz 1 Buchstabe b und hinsichtlich des Tatobjekts „Vorrichtungen“ in Absatz 1 Buchstabe b Ziffer i Gebrauch gemacht werden.

Daher wird erklärt, dass von Artikel 42 des Übereinkommens insoweit Gebrauch gemacht wird, als Artikel 6 Abs. 1 Ziffer i im Hinblick auf das Tatmittel der „Vorrichtungen“ und Buchstabe b nicht angewendet werden.

Zu Artikel 7 – Computerbezogene Fälschung

Artikel 7 enthält die Vorgabe, im Computerstrafrecht einen Straftatbestand gegen Fälschung von Computerdaten vorzusehen. Der Grund hierfür ist, dass die herkömmlichen Tatbestände gegen Urkundenfälschung nur verkörperte Urkunden erfassen und deren visuelle Lesbarkeit voraussetzen, was im Fall von elektronisch gespeicherten Daten gerade nicht gegeben ist. Da die Fälschung beweiserheblicher Daten im Rechtsverkehr vergleichbare Auswirkungen wie eine Urkundenfälschung haben kann, schützt dieser Artikel die Sicherheit und Zuverlässigkeit elektronischer Daten, die für den Rechtverkehr Folgen haben können.

Tathandlung ist das zu unechten Daten führende vorsätzliche und unbefugte Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten. Der Begriff der Echtheit bezieht sich – wie im deutschen Recht – auf die Authentizität des Verfassers/Ausstellers der „Urkunde“, nicht auf die Wahrheit des Inhalts (vgl. Nummer 82 des Erläuternden Berichts).

Subjektiv ist neben dem allgemeinen Tatvorsatz die Absicht des Täters erforderlich, dass die Daten für rechtliche Zwecke verwendet oder einer Handlung zugrunde gelegt werden, als wären sie echt.

Artikel 7 ist bereits durch § 269 StGB (Fälschung beweiserheblicher Daten) vollständig umgesetzt. Die Tathandlungen „Eingeben, Verändern, Löschen und Unterdrücken“ sind durch die Tatbestandsmerkmale „speichern“ und „verändern“ vollständig erfasst. Die unbefugte „Eingabe“ richtiger oder unrichtiger Daten führt zu einer Situation, die dem Herstellen einer falschen Urkunde entspricht. Späteres „Verändern“, „Löschen“ und „Unterdrücken“ entspricht im Allgemeinen dem Verfälschen einer echten Urkunde. Entsprechend sind die Tatmodalitäten des „Speicherns“ und „Veränderns“ bei § 269 StGB in Anlehnung an die Urkundenfälschung (§ 267 StGB) konzipiert. „Speichern“ entspricht dem Herstellen einer unechten Urkunde und damit dem „Eingeben“ des Artikels 7 des Übereinkommens. Verändern bedeutet Einwirken auf bereits vorhandene Daten mit der Folge, dass der Inhalt einer gespeicherten Gedankenerklärung durch einen anderen ersetzt und damit die Beweisrichtung geändert wird. Dies entspricht dem Verfälschen einer echten Urkunde und damit den Tatmodalitäten „Verändern“, „Löschen“ und „Unterdrücken“ des Artikels 7 des Übereinkommens.

Die Absicht, dass die Daten für rechtliche Zwecke verwendet werden oder einer Handlung zugrunde gelegt werden, als wären sie echt, ist im deutschen Recht von der Notwendigkeit des Vorsatzes hinsichtlich des Tatbestandsmerkmals der Beweiserheblichkeit abgedeckt.

Das subjektive Tatbestandsmerkmal der Täuschungsabsicht im Rechtsverkehr ist von der Einschränkungsmöglichkeit der betrügerischen oder ähnlichen unredlichen Absicht in Artikel 7 Satz 2 abgedeckt. Insoweit wird von der Einschränkungsmöglichkeit im Sinne des Artikels 40 Gebrauch gemacht.

Daher wird in Übereinstimmung mit Artikel 40 des Übereinkommens erklärt, dass von der Möglichkeit Gebrauch gemacht wird, nach Artikel 7 Satz 2 das zusätzliche Merkmal der „betrügerischen oder ähnlichen unredlichen Absicht“ in Form der „Täuschung im Rechtsverkehr“ als Voraussetzung für die nach Artikel 7 Satz 1 im deutschen Recht umschriebenen Straftat der Fälschung beweiserheblicher Daten in § 269 StGB vorzusehen.

Zu Artikel 8 – Computerbezogener Betrug

Nach Artikel 8 ist der Computerbetrug in den Vertragsstaaten unter Strafe zu stellen. Ziel ist es, unzulässige Manipulationen in Datenverarbeitungsvorgängen, die in

der Absicht vorgenommen werden, rechtswidrige Vermögensübertragungen zu bewirken, mit Strafe zu bedrohen.

Tathandlungen sind die bereits aus den voranstehenden Artikeln bekannten Tatbestandsmerkmale „Eingeben“, „Verändern“, „Löschen“ oder „Unterdrücken“ (Buchstabe a), ergänzt durch den allgemeinen Handlungstatbestand „Eingreifen in die Funktionsweise eines Computers oder Systems“ (Buchstabe b). Folge der Tathandlungen muss die Beschädigung fremden Vermögens sein, wobei dieser Begriff nicht nur den Verlust von Geld, sondern sämtlichen Vermögenspositionen mit wirtschaftlichem Wert erfasst. Sowohl die Tathandlung als auch der zu erlangende wirtschaftliche Vorteil müssen „unbefugt“ sein. Subjektiv wird neben dem allgemeinen Tatvorsatz eine betrügerische oder unredliche Absicht verlangt, die darauf gerichtet sein muss, sich oder einem Dritten einen Vermögensvorteil zu verschaffen.

Artikel 8 ist bereits durch § 263a StGB vollständig umgesetzt. Die normierten Tathandlungen sind jedenfalls durch die allgemeine Tatbestandshandlung „sonst unbefugte Einwirkung auf den Ablauf einer Datenverarbeitung“ erfasst, die zu einer Vermögensschädigung führen muss. Zum Vermögen gehören nach allgemeiner Ansicht alle Güter, soweit sie einen wirtschaftlichen Wert haben. Auch enthält § 263a StGB das subjektive Tatbestandsmerkmal der rechtswidrigen Bereicherungsabsicht.

Zu Artikel 9 – Straftaten mit Bezug zu Kinderpornographie

Artikel 9 dient der Verbesserung des Schutzes von Kindern, indem er den Vertragsstaaten vorgibt, im Rahmen der zumeist bereits bestehenden nationalen Strafvorschriften gegen Kinderpornographie die zunehmende Nutzung von Computersystemen bei der Begehung dieser Straftaten zu berücksichtigen. Entsprechend sind die in Artikel 9 aufgeführten Tathandlungen computerspezifisch ausgestaltet.

Artikel 9 Abs. 1 beschreibt verschiedene, auf Computersysteme bezogene Aspekte der Herstellung (Herstellen zum Zwecke der Verbreitung über ein Computersystem – Buchstabe a), der elektronischen Verbreitung (Anbieten und Verfügbarmachen – Buchstabe b; Verbreiten und Übermitteln – Buchstabe c) und des elektronischen Besitzes (Beschaffen für sich selbst oder einen anderen – Buchstabe d; Besitz – Buchstabe e) von Kinderpornographie.

Nach Artikel 9 Abs. 2 soll pornographisches Material dem Begriff der „Kinderpornographie“ unterfallen, wenn die visuell dargestellte Person tatsächlich minderjährig ist (a) oder dem äußeren Erscheinungsbild nach wie eine minderjährige Person aussieht (b). Dem Begriff der Kinderpornographie sollen auch real erscheinende (z. B. mittels Computer erstellte oder veränderte) Bilder unterfallen, die eine minderjährige Person bei eindeutigen sexuellen Handlungen zeigen (c). Ob die Handlungen real oder nur vorgetäuscht sind, spielt keine Rolle. Während der Erläuternde Bericht in Nummer 100 festlegt, was mindestens als „sexuell eindeutige Handlung“ anzusehen ist, bleibt die Ausgestaltung des Begriffs „pornographisches Material“ dem nationalen Recht überlassen.

Die aufgezählten Tathandlungen (Absatz 1) und -objekte (Absatz 2) sind nach geltendem Recht strafbar, soweit die pornographischen Darstellungen den sexuellen Missbrauch von Personen unter 14 Jahren zum Gegenstand haben (§ 184b i. V. m. § 11 Abs. 3 StGB). Über § 11 Abs. 3 StGB ist sichergestellt, dass der Pornographietatbestand auch auf Handlungen im Rahmen von Computersystemen anwendbar ist.

Die Einlegung des Vorbehalts nach Artikel 9 Abs. 4 hinsichtlich der Beschaffungs- und Besitzstrafbarkeit (Absatz 1 Buchstabe d und e) sowie hinsichtlich des Umfangs der kinderpornographischen Darstellungen auch auf real erscheinende Bilder und Personen mit dem Erscheinungsbild eines Minderjährigen (Absatz 2 Buchstabe b und c) ist daher nicht erforderlich. Hierzu hat der 1. Strafsenat des BGH in einer Entscheidung vom 27. Juni 2001 (Az.: 1 StR 66/01) festgestellt, dass das Tatbestandsmerkmal „sexueller Missbrauch von Kindern zum Gegenstand haben“ stets vorliegt, wenn die Person des tatsächlichen sexuellen Missbrauchs ein Kind ist; in den übrigen Fällen komme es auf die Sicht eines verständigen Betrachters an.

Als „minderjährige Person“ ist nach Artikel 9 Abs. 3 anzusehen, wer das 18. Lebensjahr noch nicht vollendet hat. Dies entspricht auch der Definition des „Kindes“ im Sinne des Übereinkommens vom 20. November 1989 der Vereinten Nationen über die Rechte des Kindes. Es kann jedoch eine bis zum 16. Lebensjahr herabgesenkte Altersgrenze vorgesehen werden.

Ein höheres Mindestalter als 14 Jahre fordern neben diesem Übereinkommen das Fakultativprotokoll vom 25. Mai 2000 zum Übereinkommen der Vereinten Nationen über die Rechte des Kindes betreffend den Verkauf von Kindern, die Kinderprostitution und die Kinderpornographie sowie der EU-Rahmenbeschluss zur Bekämpfung der sexuellen Ausbeutung von Kindern und von Kinderpornographie.

Zur Umsetzung der internationalen Verpflichtungen zum Mindestalter schlägt der Entwurf eines Gesetzes zur Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie (BT-Drs. 16/3439) vor, den Anwendungsbereich von § 184b StGB auf Schriften auszudehnen, die den sexuellen Missbrauch von, an oder vor Jugendlichen zwischen 14 und 18 Jahren zum Gegenstand haben.

Zu Artikel 10 – Straftaten in Zusammenhang mit Verletzung des Urheberrechts und verwandter Schutzrechte

Die in Artikel 10 geforderten Strafvorschriften dienen dem Schutz des geistigen Eigentums in Computersystemen. Hierdurch wird der Tatsache Rechnung getragen, dass Verletzungen von Urheberrechten und verwandten Schutzrechten zu den am häufigsten begangenen Internet-Straftaten zählen.

Die zu schaffenden Straftatbestände müssen die in gewerbsmäßigem Umfang und mittels eines Computersystems begangene vorsätzliche Verletzung von Urheberrechten (Absatz 1) und verwandten Schutzrechten (Absatz 2) unter Strafe stellen. Ausgenommen sind von dieser Verpflichtung nur die jeweiligen Urheberpersönlichkeitsrechte. Wie der Wortlaut der Absätze 1 und 2 („aufgrund ihrer Verpflichtungen“) deutlich macht, ist die Vorgabe nur verbindlich, wenn ein Staat Vertragspartei der dort genannten Übereinkommen ist und auch

keinen zulässigen Vorbehalt angebracht hat, der seine Kriminalisierungsverpflichtung einschränkt. Die Begriffe „vorsätzlich“ und „in gewerbsmäßigem Umfang“ sind an die Terminologie des Übereinkommens über handelsbezogene Aspekte der Rechte des geistigen Eigentums (TRIPS) angelehnt.

Nach Absatz 3 besteht für die Vertragsstaaten die Möglichkeit, einen Vorbehalt einzulegen und die in den Absätzen 1 und 2 vorgeschriebene strafrechtliche Verantwortlichkeit unter begrenzten Umständen nicht vorzusehen, wenn andere wirksame Abhilfen zur Verfügung stehen. In keinem Fall dürfen hierbei völkerrechtliche Verpflichtungen, insbesondere Artikel 61 TRIPS als Mindestnorm, beeinträchtigt werden.

Artikel 10 Abs. 1 und 2 ist durch die §§ 106 ff. des Urheberrechtsgesetzes bereits vollständig umgesetzt. Die dort normierten Straftatbestände sind sogar wesentlich weiter gefasst, indem auch nichtgewerbsmäßiges Handeln und der Versuch unter Strafe gestellt sind. Die von Artikel 10 in Bezug genommenen WIPO-Verträge WCT (WIPO Copyrights Treaty) und WPPT (WIPO Performances and Phonograms Treaty) sind durch Deutschland zwar noch nicht ratifiziert worden. Die notwendigen inhaltlichen Anpassungen des Urheberrechtsgesetzes sind aber bereits mit dem Gesetz vom 10. September 2003 zur Regelung des Urheberrechts in der Informationsgesellschaft, das am 13. September 2003 in Kraft trat (BGBl. I S. 1774), erfolgt.

Zu Artikel 11 – Versuch und Beihilfe oder Anstiftung

Nach Absatz 1 dieser Vorschrift müssen die Vertragsstaaten für die in den Artikeln 2 bis 10 genannten Straftaten eine Teilnahmestrafbarkeit (Beihilfe oder Anstiftung) vorsehen.

Die bestehenden Vorschriften des Allgemeinen Teils des StGB über die Teilnahme (§§ 26, 27 StGB) reichen aus, um den in Artikel 11 Abs. 1 aufgestellten Anforderungen zu genügen.

Weiterhin müssen die Vertragsstaaten nach Absatz 2 dieser Vorschrift für die in den Artikeln 3 bis 5 sowie 7, 8, 9 Abs. 1 Buchstabe a und c genannten Straftaten eine Versuchsstrafbarkeit einführen.

Mit Ausnahme der in Artikel 3 genannten Taten ist die Versuchsstrafbarkeit in allen genannten Fällen im deutschen Recht ausdrücklich normiert (vgl. Artikel 5: § 303b Abs. 2 StGB; Artikel 7: § 269 Abs. 2 StGB; Artikel 8: § 263a Abs. 2 i. V. m. § 263 Abs. 2 StGB). Die Strafbarkeit des Versuchs für die in Artikel 9 Abs. 1 Buchstabe a genannten Taten (Herstellung von Kinderpornographie) ergibt sich aus den §§ 176 ff., 182, 232 Abs. 1 Satz 2 StGB (Bringen einer Person unter 21 Jahren zu sexuellen Handlungen, durch die sie ausgebeutet wird). Durch den Entwurf eines Gesetzes zur Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie soll zudem die Schutzaltersgrenze in § 182 Abs. 1 StGB auf 18 Jahre erhöht werden. Die Strafbarkeit des Versuchs für die in Artikel 9 Abs. 1 Buchstabe c bezeichneten Taten (Verbreiten und Übermitteln) ergibt sich aus der Unternehmensstrafbarkeit des § 184b Abs. 2 StGB (Unternehmen der Fremdbesitzverschaffung). Im Übrigen wird von der Vorbehaltsmöglichkeit des Artikels 11 Abs. 3 Gebrauch gemacht.

Daher wird erklärt, dass von Artikel 42 des Übereinkommens insoweit Gebrauch gemacht wird, als dass der Versuch der Begehung der nach Artikel 3 beschriebenen Handlungen nicht als Straftat nach dem innerstaatlichen Recht umschrieben wird.

Zu Artikel 12 – Verantwortlichkeit juristischer Personen

Diese Vorschrift betrifft die Verantwortlichkeit juristischer Personen für die nach dem Übereinkommen umschriebenen Straftaten.

Artikel 12 enthält die Vorgabe, die Verantwortlichkeit einer juristischen Person vorzusehen, wenn eine natürliche Person, die eine Führungsposition innerhalb dieser juristischen Person innehat, in Ausübung ihrer Befugnisse (Absatz 1 Buchstabe a bis c) eine bestimmte Straftat zu Gunsten der juristischen Person begeht oder Anstifter oder Gehilfe hierzu ist. Die Verantwortlichkeit der juristischen Person wird in Absatz 2 auch auf Taten solcher Personen erweitert, die eine Straftat als Mitarbeiter ohne Führungsposition der juristischen Person zu deren Gunsten begehen, wenn die Begehung aufgrund mangelnder Überwachung oder Kontrolle durch eine Person in Führungsposition ermöglicht wurde.

Die Verantwortlichkeit der juristischen Personen kann strafrechtlicher oder nicht strafrechtlicher Art sein. Artikel 13 Abs. 2 schreibt aber vor, dass die Sanktionen oder Maßnahmen gegen juristische Personen wirksam, verhältnismäßig und abschreckend sein und Geldsanktionen umfassen müssen.

Mit den §§ 30, 130 OWiG besteht im deutschen Recht ein Instrumentarium, das den Anforderungen des Artikels 12 genügt. Diese Vorschriften sehen eine bußgeldrechtliche Verantwortlichkeit juristischer Personen (und anderer Personenvereinigungen) vor. Sie gilt für alle Straftaten, die von einer Leitungsperson oder – über § 130 OWiG – einem sonstigen Mitarbeiter des Verbandes begangen werden. Mit dem Gesetz vom 22. August 2002 zur Ausführung des Zweiten Protokolls vom 19. Juni 1997 zum Übereinkommen über den Schutz der finanziellen Interessen der Europäischen Gemeinschaften, der Gemeinsamen Maßnahme betreffend die Bestechung im privaten Sektor vom 22. Dezember 1998 und des Rahmenbeschlusses vom 29. Mai 2000 über die Verstärkung des mit strafrechtlichen und anderen Sanktionen bewehrten Schutzes gegen Geldfälschung im Hinblick auf die Einführung des Euro (BGBl. I S. 3387) wurde der Kreis der von § 30 OWiG erfassten natürlichen Personen erweitert. Darunter fallen auch solche Führungspersonen, die ihre Leitungsfunktion aus einer Kontrollbefugnis ableiten. Mit der durch das Einundvierzigste Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vorgenommenen Streichung der Wörter „als solchen“ in § 130 Abs. 1 Satz 1 OWiG wurde im Einklang mit der herrschenden Meinung nur klargestellt, dass § 130 OWiG nicht nur Sonderdelikte, sondern – ebenso wie § 30 OWiG – auch Allgemeindelikte erfasst, wenn sie im Zusammenhang mit der Betriebs- oder Unternehmensführung stehen.

Zu Artikel 13 – Sanktionen und Maßnahmen

Für natürliche Personen müssen die vorgesehenen strafrechtlichen Sanktionen und Maßnahmen „wirksam, verhältnismäßig und abschreckend“ sein und die Möglichkeit der Freiheitsstrafe einschließen (Absatz 1). Für juristische Personen genügen auch nichtstrafrechtliche Sanktionen oder Maßnahmen, die allerdings Geldsanktionen umfassen müssen (Absatz 2).

Aus Absatz 1 ergibt sich kein Umsetzungsbedarf. Gegen natürliche Personen ist nach den einschlägigen Straftatbeständen die Verhängung von Geldstrafe oder von Freiheitsstrafe möglich; letztere kann – je nach verwirklichter Strafvorschrift – bis zu einer Freiheitsstrafe von zehn Jahren reichen. Möglich sind weitere Sanktionen, etwa – je nach den Umständen des Einzelfalls – die Verhängung eines strafrechtlichen Berufsverbots (vgl. §§ 70 ff. StGB).

Den Anforderungen des Absatzes 2 hinsichtlich der Sanktionierung juristischer Personen wird das geltende Recht durch die Vorschrift des § 30 OWiG gerecht. § 30 Abs. 2 OWiG ermöglicht bei Straftaten als Anknüpfungstaten die Verhängung einer Geldbuße von bis zu einer Million Euro. Ist dies zur Abschöpfung des aus der Tat erlangten wirtschaftlichen Vorteils erforderlich, kann und soll dieser Betrag auch überschritten werden (§ 30 Abs. 3 i. V. m. § 17 Abs. 4 OWiG). Ergänzt werden diese bußgeldrechtlichen Regelungen durch die gewerbe- und gesellschaftsrechtlichen Möglichkeiten, die Tätigkeit des Unternehmens zu beschränken oder zu untersagen oder dessen Rechtsträger aufzulösen. Damit steht ein umfassendes Sanktionsinstrumentarium zur Verfügung.

Abschnitt 2 – Verfahrensrecht

Abschnitt 2 dient der Harmonisierung des Strafverfahrensrechts und seiner Anpassung an die veränderten technologischen Gegebenheiten. Besondere Schwierigkeiten bestehen aufgrund der Flüchtigkeit der elektronischen Daten und bei der Ermittlung des Täters. Um diesen Schwierigkeiten angemessen begegnen zu können, werden traditionelle Ermittlungsmethoden wie Durchsuchung und Beschlagnahme im Hinblick auf datenspezifische Besonderheiten modernisiert (Artikel 19), zugleich aber auch neue Maßnahmen wie die umgehende Sicherung und Herausgabe von Daten (Artikel 16, 17 und 18) oder die Echtzeit-Erfassung von Daten (Artikel 20 und 21) geschaffen.

Die Ermittlungsbefugnisse beziehen sich auf alle Arten von Computerdaten, soweit nicht nach der Art der Daten (Computerdaten, Verkehrsdaten, Inhaltsdaten und Kundendaten) unterschieden wird. Bei der Erfassung der Daten wird außerdem danach differenziert, ob diese bereits in gespeicherter Form vorliegen oder noch im Übertragungsvorgang befindlich sind.

Das deutsche Strafprozessrecht entspricht im Wesentlichen den Vorgaben des Übereinkommens. Änderungen sind nur in Teilbereichen notwendig. Anpassungsbedarf besteht lediglich im Zusammenhang mit den Artikeln 16 bis 18 und 20 im Hinblick auf die umgehende Sicherung, Weiter- und Herausgabe sowie Erhebung von Verkehrsdaten und bei Artikel 19 hinsichtlich der Erstreckung der offenen Durchsuchung auf räumlich getrennte Speichermedien.

Zu den Artikeln 14 und 15 – Geltungsbereich verfahrensrechtlicher Bestimmungen sowie Bedingungen und Garantien

Die Artikel 14 (Geltungsbereich verfahrensrechtlicher Bestimmungen) und 15 (Bedingungen und Garantien) enthalten die allgemeinen Bestimmungen zu den in den Artikeln 16 bis 21 genannten Ermittlungsmethoden. Entsprechend wird in jeder dieser anderen Vorschriften ausdrücklich darauf hingewiesen, dass die dort genannten einzelnen Befugnisse und Verfahren den Artikeln 14 und 15 unterliegen.

Artikel 14 Abs. 2 schreibt vor, dass die in den Artikeln 16 bis 21 aufgezählten Ermittlungsbefugnisse sowohl für die in den Artikeln 2 bis 11 des Übereinkommens festgelegten Straftaten als auch für andere, mittels eines Computersystems begangene Straftaten vorgesehen sein müssen. Darüber hinaus müssen diese Befugnisse allgemein auf die Erhebung von Beweisen in elektronischer Form anwendbar sein. Ausnahmen hiervon sind für die Echtzeit-Erhebung von Daten vorgesehen.

Das deutsche Strafprozessrecht erfüllt diese Vorgabe. Die Ermittlungsbefugnisse des deutschen Strafprozessrechts beziehen sich grundsätzlich auf alle Straftaten. Nur bei besonders eingriffsintensiven Ermittlungsbefugnissen werden erhöhte Anforderungen an das Gewicht der zugrunde liegenden Straftat gestellt. Da je nach Art der Eingriffsbefugnis unterschiedliche Anforderungen gestellt werden, wird hierauf im Einzelnen bei den jeweiligen Eingriffsbefugnissen eingegangen.

Artikel 15 beschreibt die Bedingungen und Garantien, die für die in den Artikeln 16 bis 21 vorgesehenen Eingriffsbefugnisse bestehen müssen. Danach sind die Vertragsparteien verpflichtet, bei der Schaffung, Umsetzung und Anwendung der genannten Befugnisse die Menschenrechte und Freiheiten angemessen zu schützen sowie dem Grundsatz der Verhältnismäßigkeit Rechnung zu tragen (Absatz 1). Hierzu gehört neben der Kontrolle dieser Befugnisse durch Gerichte oder andere unabhängige Stellen unter anderem auch die Begründung der Anwendung und eine Begrenzung im Hinblick auf Umfang und Dauer (Absatz 2). Zu den weiteren Garantien, die der Regelung durch das innerstaatliche Recht überlassen bleiben, zählen beispielsweise auch Zeugnis- und Aussageverweigerungsrechte sowie Besonderheiten bei Personen oder Orten, die Gegenstand der Maßnahme sind. Auch die Auswirkungen der Befugnisse auf Dritte sollen, soweit mit dem öffentlichen Interesse vereinbar, berücksichtigt werden (Absatz 3).

Diese Verfahrensgarantien werden vom innerstaatlichen Strafprozessrecht eingehalten. Hinzuweisen ist insbesondere darauf, dass eine gerichtliche oder sonstige unabhängige Kontrolle der Ermittlungsmaßnahmen im Sinne von Artikel 15 Abs. 2 durch einen Antrag auf gerichtliche Entscheidung (§ 98 Abs. 2 Satz 2 StPO) und den Rechtsbehelf der Beschwerde (§ 304 StPO) im deutschen Recht gewährleistet wird, die auch nach Erledigung der Maßnahme zulässig sind. Soweit gegen Verfügungen des Ermittlungsrichters des Bundesgerichtshofs und des Oberlandesgerichts eine Beschwerde nur in bestimmten Fällen zulässig ist (§ 304 Abs. 5 StPO), besteht das Recht der Gegenvorstellung. Daneben ist das Gericht befugt, die Rechtmäßigkeit der Ermittlungsmaßnahme in der Hauptverhandlung zu überprüfen.

Zu Artikel 16 – Umgehende Sicherung gespeicherter Computerdaten

Artikel 16 befasst sich mit der beschleunigten Sicherung gespeicherter Computerdaten, einschließlich Verkehrsdaten. Die Vertragsparteien werden in Absatz 1 dazu verpflichtet, ihren Behörden die Befugnis zu erteilen, die beschleunigte Sicherung bestimmter gespeicherter Computerdaten anzuordnen oder in ähnlicher Weise zu bewirken. „Sicherung“ bedeutet in diesem Zusammenhang, Daten, die bereits in gespeicherter Form existieren, gegen alles zu schützen, was ihre gegenwärtige Eigenschaft oder Beschaffenheit verändern könnte. Es handelt sich hierbei um eine vorläufige Maßnahme, die im Bereich der Computerkriminalität eine wichtige Ermittlungshilfe darstellt. Eine Sicherungsanordnung im Sinne dieser Vorschrift beinhaltet allerdings nicht, dass die Daten zum Zeitpunkt der Sicherung an die Strafverfolgungsbehörden weitergegeben werden müssen. Die Vorschrift begründet nur die Befugnis, im Zusammenhang mit besonderen strafrechtlichen Ermittlungen oder Verfahren (vgl. Artikel 14 Abs. 1) die Sicherung existierender Daten bis zu einer späteren Weitergabe der Daten aufgrund anderer gesetzlicher Befugnisse zu verlangen.

Nach Absatz 2 kann die beschleunigte Sicherung gespeicherter Computerdaten auch über andere Personen erfolgen, in deren Besitz oder Verfügungsgewalt sich die betreffenden Computerdaten befinden. In diesem Fall müssen die Vertragsparteien sicherstellen, dass diese Personen verpflichtet sind, die Integrität dieser Computerdaten so lange wie notwendig (höchstens für die Dauer von 90 Tagen) zu sichern und zu erhalten, wobei eine anschließende Verlängerung der Anordnung möglich ist.

Der Verwahrer oder eine andere Person, welche die Computerdaten zu sichern hat, müssen von den Vertragsparteien gemäß Absatz 3 zur Vertraulichkeit verpflichtet werden.

Die Beschlagnahme von Computerdaten erfolgt nach deutschem Strafverfahrensrecht durch Beschlagnahme der Datenträger, auf denen die Daten gespeichert sind. Die Vorgaben des Artikels 16 sind daher im Hinblick auf die umgehende Sicherung von Computerdaten vollständig abgedeckt durch die Regeln der Beschlagnahme in §§ 94 ff. StPO.

Das deutsche Strafprozessrecht kennt keine ausdrückliche Regelung zur bloßen Sicherung, etwa im Sinne eines „Einfrierens“, beweiserheblicher Computerdaten. Allerdings kann (als weiterreichende Maßnahme) die Herausgabe von Computerdaten erreicht werden. Möglichkeiten einer – auch beschleunigten – Sicherstellung von Computerdaten sind daher durch die Regelungen über die Beschlagnahme in den §§ 94 ff. StPO gegeben. Diese erlauben den Strafverfolgungsbehörden, auf Computerdaten unmittelbar zuzugreifen und sie auf diese Weise für ein Strafverfahren zu sichern. Wie sich aus den Nummern 155 und 160 des Erläuternden Berichts ergibt, erkennt das Übereinkommen diese Art der Beweissicherung an.

In Bezug auf Verkehrsdaten wird die Vorgabe des Artikels 16 Abs. 1 in Form des Absatzes 2 des Übereinkommens hinsichtlich des „Einfrierens“ von Verkehrsdaten durch die in dem Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vorgeschlagenen Regelungen zur sogenannten Vorratsdatenspeicherung (BT-Drs. 16/5846) vollständig abgedeckt, soweit sich die Verkehrsdaten im Gewahrsam von Diensteanbietern befinden. Nach dem darin enthaltenen Entwurfs eines § 113a des Telekommunikationsgesetzes (TKG) sind – die in der Richtlinie beschriebenen – Verkehrsdaten über einen Zeitraum von sechs Monaten zu speichern.

Im Übrigen ist die Vorgabe der – auch beschleunigten – Sicherstellung solcher Verkehrsdaten, die sich nicht im Gewahrsam eines Telekommunikationsanbieters befinden, durch die allgemeinen Regelungen über die Beschlagnahme in den §§ 94 ff. StPO abgedeckt. Eine Klarstellungsvorschrift sieht der Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG in § 100g Abs. 3 StPO vor.

Zu Artikel 17 – Umgehende Sicherung und teilweise Weitergabe von Verkehrsdaten

Artikel 17 bezieht sich als Sondervorschrift zu Artikel 16 auf die Sicherung von Verkehrsdaten. Die Vorschrift trägt der Tatsache Rechnung, dass an der Übertragung eines Kommunikationsvorganges meist mehrere Diensteanbieter beteiligt sind. Sie soll der Gefahr des Datenverlustes durch zeitlich bedingte Verzögerungen bei der Sicherungsanordnung begegnen.

Die Vertragsstaaten müssen daher sicherstellen, dass die beschleunigte Sicherung von Verkehrsdaten auch in den Fällen möglich ist, in denen mehrere Diensteanbieter an der Übertragung einer Kommunikation mitgewirkt haben. Wie dies erfolgt, bleibt allerdings ihnen überlassen; so etwa durch die Ermöglichung einer einzigen Sicherungsanordnung für den Gesamtvorgang der Kommunikationsübertragung.

Weiterhin müssen die Vertragsstaaten sicherstellen, dass der Diensteanbieter, der Adressat einer Sicherungsanordnung ist, Verkehrsdaten an Behörden oder an eine von diesen bezeichnete Person weitergibt, damit der Kommunikationsweg festgestellt werden kann.

Artikel 17 wird derzeit im Wesentlichen von § 100g StPO abgedeckt. Umsetzungsbedarf besteht aber im Hinblick auf den Personenkreis der Verpflichteten. Auskunftspflichtig sind bisher nur diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen. Eine solche Einschränkung sieht das Übereinkommen jedoch nicht vor. Nach dem Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG wird § 100g StPO neu gefasst und als umfassende Erhebungsbefugnis für Verkehrsdaten ausgestaltet (Absatz 1), wobei eine Regelung zur Auskunftspflicht beibehalten wird (Absatz 2 i. V. m. § 100b Abs. 3 StPO). Die neue Fassung sieht in Absatz 3 eine Klarstellung dahingehend vor, dass die Sicherung und Weitergabe von Verkehrsdaten – soweit sie sich nicht im Gewahrsam eines Telekommunikationsdiensteanbieters befinden – nach den allgemeinen Regelungen über die Beschlagnahme in den §§ 94 ff. StPO erfolgt. Soweit die Neufassung eine Beschränkung auf bestimmte Straftaten beibehält, steht dies nicht im Widerspruch zum Europarat-Übereinkommen. Das Erfordernis einer Straftat von auch im Einzelfall erheblicher Bedeutung

oder eine Straftat mittels Telekommunikation begangen, ist in Anbetracht der Artikel 14 und 15 möglich, wonach der Verhältnismäßigkeitsgrundsatz zu beachten ist. Zu den Einzelheiten wird auf den Gesetzentwurf verwiesen.

Zu Artikel 18 – Anordnung der Herausgabe

Diese Vorschrift regelt die sogenannte Herausgabeanordnung gegenüber einem Diensteanbieter und anderen Personen als alternative Ermittlungsmethode gegenüber dem eingriffsintensiveren Verfahren der Durchsuchung und Beschlagnahme.

Nach Absatz 1 Buchstabe a werden die Vertragsparteien verpflichtet, die Herausgabeanordnung gegenüber Personen, in deren Besitz oder Verfügungsgewalt sich bestimmte Computerdaten befinden, zu regeln. Bei den fraglichen Daten muss es sich um bereits gespeicherte und vorhandene Daten handeln. Die Maßnahme kann außerdem nur angewandt werden, wenn die betreffende Person überhaupt über solche Daten verfügt.

Absatz 1 Buchstabe b sieht vor, dass die Vertragsparteien die Herausgabeanordnung gegenüber Diensteanbietern in Bezug auf deren Kundendaten regeln. Die Definition von „Kundendaten“ enthält Absatz 3. Man versteht hierunter beim Diensteanbieter über den Teilnehmer in Daten- oder anderer Form vorliegende Informationen (außer Inhalts- und Verkehrsdaten), mit denen die in Absatz 3 Buchstabe a bis c genannten Tatsachen festgestellt werden können. „Teilnehmer“ soll nach dem Erläuternden Bericht (vgl. Nummer 177) einen großen Kreis von Kunden des Diensteanbieters einschließen, von Beitragszahlern über diejenigen, die pro Nutzung zahlen, bis zu denen, die Dienste kostenlos in Anspruch nehmen. Eingeschlossen sein sollen auch Personen, die berechtigt sind, das Kundenkonto zu nutzen. Der Diensteanbieter muss hierbei nur solche Kundendaten vorlegen, die in Zusammenhang mit seinem Dienst und ihm auch zur Verfügung stehen. Die Vorschrift ist dagegen nicht so zu verstehen, als sei der Diensteanbieter verpflichtet, überhaupt Unterlagen über seine Kunden zu führen oder die Richtigkeit solcher Angaben (etwa durch Identitätsprüfung des Kunden) zu gewährleisten (vgl. Nummer 181 des Erläuternden Berichts).

Der Vorgabe des Artikels 18 Abs. 1 Buchstabe a ist im deutschen Recht durch § 95 StPO Rechnung getragen. Diese Vorschrift regelt die Verpflichtung einer Person, die nicht Beschuldigte ist, einen Gegenstand, der sich in ihrem Gewahrsam befindet, auf Erfordern der Strafverfolgungsbehörden vorzulegen und auszuliefern. Die Vorschrift bezieht sich – ihrem Wortlaut nach – auf körperliche Sachen, wird aber auf Computerdaten entsprechend angewandt.

Die Herausgabepflicht von Diensteanbietern i. S. v. Artikel 18 Abs. 1 Buchstabe b findet sich im deutschen Recht in § 112 Abs. 2 und 4 (automatisiertes Auskunftsverfahren) und § 113 TKG (manuelles Auskunftsverfahren). Im automatisierten Auskunftsverfahren haben Unternehmen und Personen, die Telekommunikationsdienste für die Öffentlichkeit erbringen, den Gerichten und Strafverfolgungsbehörden Auskünfte aus den Kundendateien zu erteilen, soweit die Auskünfte zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind und die Ersuchen an die Regulierungsbehörde im automatisierten Verfahren vorgelegt werden. Kundendateien enthalten nach geltendem Recht folgende Daten: Rufnummer, Name und Anschrift des Rufnummerninhabers, Datum des Vertragsbeginns, ggf. Geburtsdatum, ggf. Anschrift des Anschlusses vor der Freischaltung, Änderungen (vgl. § 111 Abs. 1 Satz 1 und 3 TKG). Der Entwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG sieht ergänzend die Speicherung anderer Anschlusskennungen sowie in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, der Gerätenummer dieses Gerätes vor. Sofern Anbieter der elektronischen Post die Namen, Anschriften und Postfachkennungen ihrer Kunden erheben, sieht der Entwurf auch insoweit eine Pflicht zur Speicherung der Daten für die Auskunftsverfahren nach §§ 112, 113 TKG vor. Im manuellen Auskunftsverfahren muss jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, im Einzelfall den zuständigen Stellen auf deren Verlangen unverzüglich Auskünfte über die von ihm nach § 111 TKG erhobenen Daten erteilen, soweit dies unter anderem für die Verfolgung von Straftaten oder Ordnungswidrigkeiten erforderlich ist.

Zu Artikel 19 – Durchsuchung und Beschlagnahme gespeicherter Computerdaten

Artikel 19 befasst sich mit der Durchsuchung und Beschlagnahme gespeicherter Computerdaten. Er verfolgt den Zweck, die in den Rechtsordnungen der Vertragsparteien zumeist bestehenden Regelungen zur „traditionellen“ Durchsuchung und Beschlagnahme zu modernisieren. Durch zusätzliche verfahrensrechtliche Bestimmungen soll sichergestellt werden, dass Computerdaten auf ebenso wirksame Weise beschlagnahmt werden können wie physische Gegenstände.

Die Absätze 1 und 2 befassen sich mit der Durchsuchung. Absatz 1 verpflichtet die Vertragsparteien, Eingriffsbefugnisse zur Durchsuchung eines Computersystems, eines Teils davon sowie der darin gespeicherten Computerdaten und eines Computerdatenträgers, auf dem Computerdaten gespeichert sein können, zu schaffen. Definitionen der Begriffe „Computersystem“ und „Computerdaten“ enthält Artikel 1 Buchstabe a und b. Da die hier genannten Computerdatenträger nicht notwendigerweise zu einem Computersystem gehören müssen, sondern es sich dabei auch um Speichermedien handeln kann, die sich in der unmittelbaren Umgebung des Computersystems befinden, werden sie hier zusätzlich aufgezählt. Absatz 1 gibt vor, eine umfassende Durchsuchungsbefugnis zu schaffen.

Der Begriff der Durchsuchung wird hier durch „in ähnlicher Weise darauf Zugriff nehmen“ ergänzt. Diese Formulierung soll verdeutlichen, dass im Sinne der modernen Computerterminologie die Durchsuchung von Daten auch deren Prüfung einschließt.

Absatz 2 der Vorschrift regelt den Fall der Ausweitung einer Durchsuchung auf ein anderes Computersystem, in dem sich die gesuchten Daten befinden könnten, die von dem ersten System aus rechtmäßig zugänglich und verfügbar sind. Auch diesen Fall muss das innerstaatliche Recht vorsehen. Wie eine solche Ausweitung genehmigt oder durchgeführt werden soll, überlässt das Übereinkommen allerdings dem innerstaatlichen Recht.

Absatz 3 befasst sich mit der Beschlagnahme von Computerdaten. Die Formulierung „oder in ähnlicher Weise sicherstellen“ weist auch hier darauf hin, dass eine Beschlagnahme von Daten nicht nur in der Wegnahme eines physischen Mediums, auf dem die Daten gespeichert sind, besteht. Die für die Datenbeschlagnahme notwendigen Befugnisse werden in Absatz 3 Satz 2 Buchstabe a bis d aufgezählt. Festzuhalten ist hierbei, dass die Sicherstellung von Daten in keinem Fall eine endgültige Löschung der beschlagnahmten Daten beinhaltet.

Absatz 4 der Vorschrift sieht mit der Befugnis zur Einholung von Auskünften bei auskunftspflichtigen Personen eine weitere Zwangsmaßnahme vor, die die Durchsuchung von gespeicherten Computerdaten erleichtern soll. Die Anordnung der Auskunftserteilung ist allerdings auf die „notwendigen Auskünfte“ und auf ein „vernünftiges Maß“ beschränkt.

Ein von Artikel 19 nicht geregelter Punkt ist die Frage, ob die betroffene Person von der Durchführung der Durchsuchung und Beschlagnahme benachrichtigt werden muss. Die Klärung dieser Frage hat das Übereinkommen bewusst dem innerstaatlichen Recht überlassen.

Die in Artikel 19 Abs. 1 und 3 vorgesehenen Maßnahmen der Durchsuchung und Beschlagnahme gespeicherter Computerdaten sind nach den §§ 94 ff. und 161, 163 StPO möglich.

Die nach Artikel 19 Abs. 2 zu schaffende Möglichkeit, im Rahmen der „Durchsuchung“ eines Computersystems die Maßnahme rasch auf solche beweiserheblichen Daten auszudehnen, die von dem durchsuchten Computer aus rechtmäßig zugänglich und in einem anderen Computersystem im jeweiligen Hoheitsgebiet gespeichert sind, wird durch den Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG umgesetzt. Dieser sieht eine Änderung des § 110 StPO vor. Der neue Absatz 3 erlaubt, die Durchsicht elektronischer Datenträger auf räumlich getrennte Speichereinheiten zu erstrecken, auf denen der Betroffene den Zugriff zu gewähren berechtigt ist, und Daten, die für die Untersuchung von Bedeutung sein können, zu speichern, wenn bis zur Sicherstellung der Datenträger ihr Verlust zu besorgen ist.

Die in Artikel 19 Abs. 3 Buchstabe d vorgesehene Ermächtigung der Behörden, Computerdaten in dem Computersystem, auf das Zugriff genommen wurde, unzugänglich zu machen oder sie daraus zu entfernen, ist im Lichte von Artikel 15 dahingehend zu verstehen, dass hiervon nicht jegliches in elektronischer Form sichergestelltes Beweismaterial betroffen ist, sondern nur solche Daten unzugänglich gemacht oder entfernt werden dürfen, die durch eine Straftat hervorgebracht oder zu ihrer Begehung oder Vorbereitung gebraucht worden oder bestimmt gewesen sind. Diesem Bedürfnis tragen im deutschen Recht die Vorschriften über die Sicherstellung (§§ 111b ff. StPO) und Einziehung (§§ 74 ff. StGB) Rechnung.

Die in Artikel 19 Abs. 4 vorgesehene Inanspruchnahme Dritter richtet sich im deutschen Recht nach den für Zeugen geltenden Regelungen (§§ 48 ff. StPO), die auch Zwangsmaßnahmen bei Verweigerung der Auskunft vorsehen (§ 70 StPO). Für den EDV-Bereich bedeutet dies, dass Zeugen den Ermittlungsbehörden insbesondere Informationen über Verschlüsselungstechniken, Sicherungsmechanismen oder sonstige Zugangsberechtigungen zu einem Computersystem bekannt geben müssen, soweit sie ihnen selbst bekannt sind. Im Übrigen lassen sich durch Fragen Informationen darüber gewinnen, wo sich Beweismittel (z. B. Kryptoschlüssel) befinden und wie sie zu verwerten sind. Auf der Grundlage dieser Kenntnisse können dann weitere Zwangsmaßnahmen durchgeführt werden. Etwaige Zeugnisverweigerungsrechte dieser Personen (§§ 52 ff. StPO), die im deutschen Recht zu beachten sind und eine Inanspruchnahme dieser Personen ausschließen können, dürfen gemäß Artikel 15 Abs. 1 berücksichtigt werden (vgl. Sanchez-Hermosilla, CR 2003, 774, 777 f.). Der Beschuldigte, der sich zu dem gegen ihn gerichteten Vorwurf nicht einlassen muss, kann nicht Zeuge sein.

Zu den Artikeln 20 und 21 – Erhebung von Verkehrs- und Inhaltsdaten in Echtzeit

Diese beiden Artikel schreiben die Möglichkeit der Echtzeit-Erhebung von Inhaltsdaten (Artikel 21) und Verkehrsdaten vor, die mit bestimmten, mittels eines Computersystems übertragenen Kommunikationen im Zusammenhang stehen (Artikel 20).

Der Begriff der „Verkehrsdaten“ ist hierbei in Artikel 1 Buchstabe d des Übereinkommens definiert. Im Gegensatz hierzu beziehen sich „Inhaltsdaten“ auf den Inhalt der Kommunikation. Sie sind alles, was als Bestandteil der Kommunikation übermittelt wird und keine Verkehrsdaten darstellt.

Beide Vorschriften regeln die Erhebung von Beweisdaten in „Echtzeit“. Dies bedeutet, dass die Daten im Zeitpunkt der Kommunikation erhoben werden. Rein technisch geschieht dies durch Anfertigung einer Aufzeichnung.

Beide Vorschriften enthalten vom Ansatz her gleiche Regelungen. Vor dem Hintergrund, dass nach der Auffassung vieler Staaten die Belange der Privatsphäre bei Inhaltsdaten wegen der Art des Kommunikationsinhalts und der Nachricht eine größere Rolle spielen, dürfen der Echtzeit-Erhebung von Inhaltsdaten im Vergleich zu Verkehrsdaten jedoch größere Beschränkungen auferlegt werden. Diese Ermittlungsmaßnahme ist daher auf eine „Reihe schwerer Straftaten, die nach innerstaatlichem Recht zu bestimmen sind“, beschränkt (vgl. Artikel 21). Macht ein Vertragsstaat allerdings von der nach Artikel 14 Abs. 3 des Übereinkommens bestehenden Vorbehaltsmöglichkeit bei der Echtzeit-Erhebung von Verkehrsdaten Gebrauch, so darf die Reihe von Straftaten oder die Arten von Straftaten, bei denen eine Echtzeit-Erhebung von Verkehrsdaten zulässig ist, nicht enger gefasst sein als die Reihe der Straftaten, bei denen eine Echtzeit-Erhebung von Inhaltsdaten zulässig ist.

Nach den Artikeln 20 und 21 werden die Vertragsparteien verpflichtet, ihren zuständigen Behörden die Befugnis zu erteilen, Verkehrsdaten und Inhaltsdaten durch Anwendung technischer Mittel selbst zu erheben oder aufzuzeichnen (Absatz 1 Buchstabe a). Die Vertragsparteien sind darüber hinaus aber auch verpflichtet sicherzustellen, dass ihre zuständigen Behörden befugt sind, einen Diensteanbieter zu verpflichten, Verkehrs- oder Inhaltsdaten (im Rahmen zur Verfügung stehender technischer Mittel) zu erheben oder aufzuzeichnen oder hierbei mit den zuständigen Behörden zusammenzu-

arbeiten und diese zu unterstützen (Absatz 1 Buchstabe b). Vorgeschrieben ist damit die Verfügbarkeit beider Methoden. Ist ein Staat aufgrund bestehender Vorschriften nicht in der Lage, die Daten durch seine Behörden selbst zu erheben oder aufzuzeichnen, so muss er die Erhebung oder Aufzeichnung in anderer Weise sicherstellen, etwa indem Diensteanbieter verpflichtet werden, die für die Echtzeit-Erhebung erforderliche technische Ausrüstung bereitzustellen (Absatz 2).

In jedem Fall müssen die Vertragsparteien einen Diensteanbieter verpflichten, die Eingriffsmaßnahme sowie hierdurch erlangte Informationen vertraulich zu behandeln (Absatz 3).

Die §§ 100a, 100b StPO erlauben unter strengen Voraussetzungen die Überwachung und Aufzeichnung der Telekommunikation in Echtzeit. Nach bisheriger Gesetzeslage unterscheiden die §§ 100a, 100b StPO hierbei nicht zwischen Telekommunikationsverkehrsdaten und dem Inhalt von Telekommunikation. Nach dem Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG wird der § 100g StPO nicht mehr allein als Regelung eines Auskunftsanspruchs gegenüber Telekommunikationsanbietern, sondern als umfassende Erhebungsbefugnis für Verkehrsdaten ausgestaltet.

Ist die Überwachung der Telekommunikation nach den §§ 100a, 100b StPO angeordnet, hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft oder ihren im Polizeidienst tätigen Ermittlungspersonen die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen und hierfür gegebenenfalls entsprechend den gesetzlichen Bestimmungen technische und organisatorische Vorkehrungen zu treffen (vgl. § 100b Abs. 3 StPO). Im Falle der Weigerung können Ordnungs- und Zwangsmittel festgesetzt werden (§§ 100b Abs. 3 Satz 3 i. V. m. § 95 Abs. 2 StPO). Die Strafverfolgungsbehörden sind auch berechtigt, die Überwachung ausschließlich mit eigenen Mitteln durchzuführen. § 100a Abs. 1 Satz 1 StPO erhält nach dem Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG die nicht durch die Mitwirkung des Telekommunikationsdienstleisters bedingte Befugnis, Telekommunikation zu überwachen und aufzuzeichnen.

Mitwirkungspflichtig sind bisher nur diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen. Eine solche Einschränkung sieht das Übereinkommen aber auch in diesem Bereich nicht vor. Nach dem Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG ist die Mitwirkungspflicht daher nicht mehr auf Telekommunikationsdiensteanbieter beschränkt, die ihre Dienste geschäftsmäßig erbringen.

Als besonders eingriffsintensive Maßnahme der deutschen Strafprozessordnung ist die Echtzeit-Erhebung von Telekommunikationsdaten (§§ 100a, 100b StPO) an bestimmte „Katalogtaten“ geknüpft. Dies ist im Hinblick auf Artikel 14 Abs. 2 jedoch unproblematisch, weil die Echtzeit-Erhebung von Inhaltsdaten nach Artikel 21 auf schwere Straftaten beschränkt werden darf.

Die Echtzeit-Erhebung von Telekommunikationsverkehrsdaten im Sinne des Übereinkommens ist dagegen nach der durch den Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG beabsichtigten Neufassung des § 100g StPO-Entwurfs immer dann zulässig, wenn es sich um Straftaten von auch im Einzelfall erheblicher Bedeutung, insbesondere eine der in § 100a Abs. 2 StPO genannten Straftaten, oder Straftaten, die mittels Telekommunikation begangen worden sind, handelt. Die Echtzeit-Erhebung von Standortdaten soll nach dem Entwurf allerdings lediglich bei Straftaten von erheblicher Bedeutung zulässig sein.

Von der in Artikel 14 Abs. 3 Buchstabe a vorgesehenen Vorbehaltsmöglichkeit für die Echtzeit-Erhebung von Verkehrsdaten nach Artikel 20, die auf bestimmte Straftaten oder auf Kategorien von Straftaten beschränkt werden darf, muss somit nach der Neuregelung kein Gebrauch gemacht werden. Hinsichtlich der Einzelheiten kann hier auf den Gesetzentwurf verwiesen werden.

Abschnitt 3 – Gerichtsbarkeit

Zu Artikel 22 – Gerichtsbarkeit

Artikel 22 schreibt vor, in welchen Fällen die Vertragsparteien ihre Strafgerichtsbarkeit für die in den Artikeln 2 bis 11 genannten Straftaten vorsehen müssen.

- Absatz 1 Buchstabe a umschreibt dabei das Territorialitätsprinzip,
- Absatz 1 Buchstabe b und c das Flaggenprinzip und
- Absatz 1 Buchstabe d das aktive Personalitätsprinzip.

Absatz 3 enthält das Prinzip „aut dedere aut iudicare“ bei Straftaten von Staatsangehörigen der ersuchten Vertragspartei.

Wie sich aus Absatz 4 ergibt, können die Vertragsparteien bei der Begründung ihrer Strafgerichtsbarkeit natürlich über die hier genannten Kriterien hinausgehen.

Vorbehaltsmöglichkeiten existieren für Absatz 1 Buchstabe b bis d, nicht dagegen für Absatz 1 Buchstabe a und Absatz 3.

Das Territorialitätsprinzip (Absatz 1 Buchstabe a) ist in § 3 StGB und das Flaggenprinzip (Absatz 1 Buchstabe b und c) in § 4 StGB verankert, die auch für die Strafvorschriften gelten, mit denen die Vorgaben dieses Übereinkommens in das deutsche Strafrecht umgesetzt werden. Ebenso verhält es sich mit § 7 Abs. 2 Nr. 1 StGB für das aktive Personalitätsprinzip (Absatz 1 Buchstabe d). Von der letztgenannten Vorschrift wird auch Absatz 3 erfasst, für den es deshalb keiner besonderen Umsetzungsvorschrift bedarf. Es besteht demnach kein Anlass für einen Vorbehalt nach Absatz 2.

Absatz 5 regelt den Fall, dass mehrere Vertragsparteien die Gerichtsbarkeit für eine bestimmte Straftat gleichzeitig für sich geltend machen und sieht dafür Konsultationen vor. Wie das Wort „gegebenenfalls“ nahelegt, ist die Verpflichtung zur gegenseitigen Konsultation aber nicht zwingend.

Kapitel III
Internationale Zusammenarbeit

Kapitel III des Übereinkommens enthält Regeln zur beschleunigten und vereinfachten Internationalen Zusammenarbeit bei der Verfolgung von Computerstraftaten und von Delikten, bei denen in elektronischer Form vorliegende Beweise zu erheben sind. Diese Regelungen ermöglichen keine eigenständigen Ermittlungen von Strafverfolgungsbehörden in Datennetzen im Ausland, die unzulässig bleiben (vgl. auch Artikel 32). Die Regelungen stehen in einem korrespondierenden Zusammenhang mit den Regelungen des Kapitels II über Eingriffsbefugnisse.

Die Rechtshilferegeln des Kapitels III sind bereits heute umfassend im nationalen deutschen Recht verwirklicht. Auf der Grundlage des Gesetzes über die Internationale Rechtshilfe in Strafsachen (IRG) und den diesem Gesetz vorgehenden völkerrechtlichen Vereinbarungen können Rechtshilfeersuchen gestellt und erledigt werden. Die besonderen Regelungen, welche dieses Übereinkommen enthält, können dabei umfassend eingehalten werden.

Besondere nationale Ausführungsvorschriften zu den allgemeinen Grundsätzen und den ergänzenden Regelungen dieses Kapitels sind nicht erforderlich. Für die vertragslose Rechtshilfe enthält das IRG ausreichende Ermächtigungsgrundlagen.

Die Vorschriften lehnen sich im Einzelnen zum Teil an die Artikel 7 ff. des Europarat-Übereinkommens über Geldwäsche sowie Ermittlungen, Beschlagnahme und Einziehung von Erträgen aus Straftaten (ETS Nr. 141) und die Artikel 25 ff. des Strafrechtsübereinkommens des Europarats über Korruption (ETS Nr. 173) an.

Zu Artikel 23 – Allgemeine Grundsätze der internationalen Zusammenarbeit

Diese Vorschrift enthält allgemeine Grundsätze der internationalen Zusammenarbeit. Zum einen sollen die Vertragsparteien auf internationaler Ebene „in größtmöglichem Umfang“ miteinander kooperieren. Der Umfang der Kooperationsverpflichtungen erstreckt sich hierbei auf alle Straftaten, die Computersysteme und -daten betreffen, sowie auf die Erhebung von Beweismitteln, die in elektronischer Form vorliegen (vgl. Artikel 14 Abs. 2 des Übereinkommens). Schließlich ergibt sich aus Artikel 23, dass die Verpflichtung der Vertragsparteien zur internationalen Zusammenarbeit im größtmöglichen Umfang nur in den Grenzen ihres jeweiligen nationalen Rechts und einschlägiger völkerrechtlicher Vereinbarungen besteht. Ein Gesetzgebungsbedarf kann aus dieser Vorschrift somit nicht entstehen. Soweit keine völkerrechtlichen Vereinbarungen vorgehen, ist in Deutschland die internationale Zusammenarbeit in strafrechtlichen Verfahren im IRG umfassend geregelt.

Zu Artikel 24 – Auslieferung

Die Absätze 1 und 2 sollen sicherstellen, dass eine Auslieferung wegen der in den Artikeln 2 bis 11 des Übereinkommens festgelegten Straftaten in allen Vertragsstaaten grundsätzlich, d. h. nach Maßgabe des nationalen und internationalen Rechts (vgl. Absatz 5) möglich ist. Dazu wird, soweit in dieser Hinsicht das Recht eines Vertragsstaates lückenhaft sein sollte, eine entsprechende Ergänzung des innerstaatlichen und völkervertraglichen Auslieferungsrechts vorgenommen. Diese Regelungen sind für Deutschland ohne Bedeutung, da nach deutschem Recht eine Auslieferung nach den für Deutschland geltenden multilateralen und bilateralen Vereinbarungen und nach den §§ 2 und 3 IRG möglich ist.

Auslieferungsfähig sind die in den Artikeln 2 bis 11 des Übereinkommens festgelegten Straftaten, soweit sie nach dem Recht beider Vertragsparteien mit einer Freiheitsstrafe im Höchstmaß von mindestens einem Jahr Freiheitsstrafe bedroht sind (vgl. Absatz 1 Buchstabe a). Eine sich aus einem Auslieferungsvertrag oder aus einer Vereinbarung zwischen zwei oder mehreren Vertragsparteien auf der Grundlage einheitlicher oder gegenseitiger Rechtsvorschriften ergebende andere Mindesthöchststrafe geht dem allerdings vor (vgl. Absatz 1 Buchstabe b). Da die Vorschriften des deutschen Strafrechts, die den in den Artikeln 2 bis 11 des Übereinkommens genannten entsprechen (siehe oben zu Kapitel II Abschnitt 1), alle im Höchstmaß mit mindestens einem Jahr Freiheitsstrafe bedroht sind, sind die Vorgaben im deutschen Recht erfüllt.

Absatz 3 bezieht sich auf Staaten, die im Gegensatz zur Bundesrepublik Deutschland nach ihrem innerstaatlichen Recht auf vertragsloser Grundlage nicht ausliefern dürfen. Diesen wird es durch das Übereinkommen ermöglicht, eine ausreichende Grundlage für die Auslieferung wegen der in diesem Übereinkommen genannten Straftaten zu haben.

Absatz 6 enthält den Grundsatz „aut dedere aut iudicare“. Eine Vertragspartei, die eine Auslieferung ablehnt, weil die auszuliefernde Person ein eigener Staatsangehöriger ist oder weil sie der Auffassung ist, dass sie für die Verfolgung der Straftat zuständig ist, muss die Strafverfolgung – allerdings nur auf Ersuchen der anderen Vertragspartei – selbst vornehmen. Diese Vorgabe wird durch das deutsche Recht erfüllt. Artikel 16 Abs. 2 des Grundgesetzes verbietet grundsätzlich die Auslieferung deutscher Staatsangehöriger. In diesen Fällen lässt aber § 7 Abs. 2 Nr. 1 StGB die Strafverfolgung zu.

Die Benennung einer Behörde gegenüber dem Generalsekretär des Europarats, die für die Stellung oder Entgegennahme eines Ersuchens um Auslieferung oder um vorläufige Inhaftierung zuständig ist, dient der Information der einzelnen Vertragsparteien im vertragslosen Auslieferungsverkehr. Da der diplomatische Geschäftsweg im vertragslosen Auslieferungsverkehr beachtet werden muss, beabsichtigt die Bundesregierung, bei der Ratifizierung das Auswärtige Amt unter Hinweis auf den einzuhaltenden Geschäftsweg als Zentralbehörde zu benennen.

Zu Artikel 25 – Allgemeine Grundsätze der Rechtshilfe

Artikel 25 enthält die allgemeinen Grundsätze der Rechtshilfe. Wie bereits aus Artikel 23 hervorgeht, leisten die Vertragsparteien einander dem Grundsatz nach im größtmöglichen Umfang Rechtshilfe. Diese erstreckt sich auf die in Artikel 14 Abs. 2 genannten Fälle.

Jede Vertragspartei ist nach Absatz 2 verpflichtet, die Voraussetzungen zu schaffen, um den in den Artikeln 27 bis 35 enthaltenen Bestimmungen für Rechtshilfeverfahren zu genügen. Artikel 25 enthält zwar zahlreiche Vorga-

ben, stellt aber keine Ermächtigungsgrundlage zur Rechtshilfe im Einzelfall dar. Im Grundsatz richtet sich die Rechtshilfe nach den im Recht der ersuchten Vertragspartei oder in anwendbaren Rechtshilfeverträgen vorgesehenen Bedingungen (Absatz 4). Dies gilt jedoch nur, sofern „in den Artikeln dieses Kapitels nicht ausdrücklich etwas anderes vorgesehen ist“. Umsetzungsbedarf besteht aber nicht. Aufgrund der Rahmenbeschlüsse im Bereich der Mitgliedstaaten der Europäischen Union zur Rechtshilfe, bi- und multilaterale Rechtshilfeverträge, die für die Bundesrepublik Deutschland als Vertragspartei gelten, und der Regeln über den vertragslosen Rechtshilfeverkehr nach dem IRG bestehen umfassende Regelungen, die auch die Vorgaben dieses Übereinkommens erfüllen.

Absatz 3 erlaubt in dringenden Fällen den Einsatz schneller Kommunikationsmittel und trägt damit der Tatsache Rechnung, dass Rechtshilfeersuchen in Bezug auf Computerdaten bedingt durch deren Flüchtigkeit einer beschleunigten Behandlung bedürfen können.

Absatz 5 definiert, was unter der beiderseitigen Strafbarkeit zu verstehen ist. Danach ist ausreichend, dass die Handlung, die der Straftat zugrunde liegt, wegen der um Rechtshilfe ersucht wird, auch nach dem Recht der ersuchten Vertragspartei eine Straftat ist. Unschädlich ist also, dass die Straftat einer anderen Gruppe von Straftaten zugeordnet ist oder anders umschrieben wird. Die Regelung entspricht der Rechtsprechung und Praxis in Deutschland, soweit bei der strafrechtlichen Zusammenarbeit die beiderseitige Strafbarkeit Zulässigkeitsvoraussetzung ist.

Zu Artikel 26 – Unaufgeforderte Übermittlung von Informationen

Artikel 26 erfasst die einseitige spontane Informationsübermittlung an eine andere Vertragspartei und ist für diejenigen Staaten von Bedeutung, nach deren Recht ohne vorheriges Ersuchen keine Rechtshilfe geleistet werden darf. Eine Pflicht zur unaufgeforderten Übermittlung von Informationen besteht allerdings nicht. Die Offenbarung schließt auch nicht aus, dass die übermittelnde Vertragspartei selbst ein Verfahren bezüglich der betreffenden Informationen durchführt. Anzuwenden sind die jeweiligen innerstaatlichen Bestimmungen über die Weitergabe der erforderlichen Auskünfte. Bei der Unterrichtung von ausländischen Behörden durch deutsche Stellen und der Übermittlung der erforderlichen Informationen handelt es sich um die Unterstützung eines ausländischen Verfahrens und damit um Rechtshilfe ohne vorausgegangenes Ersuchen. Gesetzliche Grundlage hierfür ist in Deutschland § 61a IRG (ergänzt durch § 83j IRG im Verkehr mit Mitgliedstaaten der EU). Umsetzungsbedarf besteht nicht.

Zu Artikel 27 – Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte

Artikel 27 enthält in seinen Absätzen 2 bis 9 eine Reihe von Regeln für die Leistung von Rechtshilfe in den Fällen, in denen zwischen den Vertragsparteien kein Rechtshilfevertrag oder eine entsprechende Vereinbarung in Kraft ist (vertragsloser Rechtshilfeverkehr). Zudem können die Vertragsparteien an Stelle eines bestehenden Rechtshilfevertrags oder einer entsprechenden Vereinbarung aber auch beschließen, die Vorschriften in den Absätzen 2 bis 9 ganz oder teilweise anzuwenden. Die Regelungen in den Absätzen 2 bis 9 sind nicht abschließend; sofern bestimmte Punkte nicht geregelt sind, gilt Artikel 25 Abs. 4 des Übereinkommens, wonach sich die Modalitäten der Rechtshilfe nach dem Recht der ersuchten Vertragspartei richten. In Deutschland richtet sich im vertragslosen Verkehr die Rechtshilfe nach dem IRG. §§ 59 ff. IRG gestattet es deutschen Justizbehörden grundsätzlich in weitem Umfang, sogenannte „sonstige“ Rechtshilfe zu leisten. Eine besondere Umsetzung ist nicht erforderlich.

Zur Erleichterung des Rechtshilfeverkehrs müssen die Vertragsparteien eine oder mehrere zentrale Behörden benennen, die zum Zwecke der Rechtshilfe unmittelbar miteinander verkehren. Bezeichnung und Anschrift dieser Behörde(n) sind dem Generalsekretär des Europarats zu notifizieren (Absatz 2). Im Hinblick auf den diplomatischen Geschäftsweg, der bei solchen Ersuchen einzuhalten ist, beabsichtigt die Bundesregierung als zentrale Behörde das Auswärtige Amt unter Hinweis auf den einzuhaltenden diplomatischen Geschäftsweg gegenüber dem Europarat zu benennen.

Die Erledigung der Rechtshilfeersuchen richtet sich grundsätzlich nach den von der ersuchenden Vertragspartei bezeichneten Verfahren. Etwas anderes gilt nur, wenn diese mit den Rechtsvorschriften der ersuchten Vertragspartei unvereinbar sind (Absatz 3). Die bloße Tatsache, dass das Rechtssystem des ersuchten Vertragsstaats das von der ersuchenden Vertragspartei benannte Verfahren nicht kennt, ist aber kein ausreichender Grund, die Anwendung dieses Verfahrens zu verweigern.

Absatz 4 enthält zusätzliche Ablehnungsgründe zu den in Artikel 25 Abs. 4 des Übereinkommens bereits genannten und auch hier anwendbaren Gründen. Die Rechtshilfe kann danach abgelehnt werden, wenn es sich nach Auffassung der ersuchten Vertragspartei bei der im Ersuchen bezeichneten Straftat um eine politische oder mit einer solchen zusammenhängenden Straftat handelt oder wenn durch die Erledigung des Ersuchens nach Auffassung des ersuchten Staates bestimmte wesentliche Interessen des Landes beeinträchtigt würden. Durch die Möglichkeit der Ablehnung der Rechtshilfe wegen der Beeinträchtigung wesentlicher Interessen des Landes ist gewährleistet, dass auch elementare Gesichtspunkte des Datenschutzes geltend gemacht werden können. Vor dem Hintergrund, dass Ausnahmetatbestände aufgrund des Grundsatzes größtmöglicher Kooperation zurückhaltend auszulegen sind, stellen jedoch weder die bloße Tatsache unterschiedlicher Datenschutzsysteme noch unterschiedlicher Möglichkeiten zum Schutze personenbezogener Daten für sich gesehen “wesentliche Interessen“ im Sinne dieser Vorschrift dar (vgl. Nummer 269 des Erläuternden Berichts). In solchen Fällen besteht die Möglichkeit, nach Absatz 6 dieser Vorschrift Bedingungen an die Übersendung der Daten zu stellen.

Absatz 5 benennt die Umstände, nach denen die ersuchte Vertragspartei die im Rechtshilfeersuchen genannten Maßnahmen aufschieben darf. Auch diese Umstände sind im Lichte des Übereinkommens eng auszulegen. Als mildere Mittel gegenüber der Ablehnung oder des Aufschubs eines Rechtshilfeersuchens sieht Absatz 6 die teilweise Erledigung oder die Stellung von

Bedingungen vor. Auch hiervon ist im Sinne des Übereinkommens zurückhaltend Gebrauch zu machen.

Die ersuchte Vertragspartei ist verpflichtet, die ersuchende Vertragspartei über das Ergebnis des Ersuchens zu unterrichten und eine Ablehnung oder einen Aufschub der Rechtshilfe zu begründen (Absatz 7). Für die sonstige Rechtshilfe im vertragslosen Verkehr trifft § 61 Abs. 1 Satz 3 i. V. m. §§ 32, 33 Abs. 4 IRG eine entsprechende Regelung zur Begründungspflicht. Regelungen für die vertrauliche Behandlung des Vorliegens eines Rechtshilfeersuchens enthält Absatz 8. Von Absatz 2 abweichende Übermittlungs- und Kommunikationsmodalitäten für Rechtshilfeersuchen in dringenden Fällen werden in Absatz 9 genannt.

Zu Artikel 28 – Vertraulichkeit und Beschränkung der Verwendung

Diese Vorschrift regelt die Verwendung von Informationen oder Unterlagen, die nach Auffassung der ersuchten Vertragspartei als vertraulich eingestuft werden, und schafft damit Garantien, die unter anderem zu Datenschutzzwecken zur Verfügung stehen. Dabei ist es besonders der Initiative Deutschlands zu verdanken, dass erstmals in einem Übereinkommen außerhalb der Europäischen Union eine Vorschrift geschaffen wurde, die auch den Schutz persönlicher Daten beim Rechtshilfeverkehr umfasst. Sie ermöglicht es dem ersuchten Staat, eine Zweckbindung und die Vertraulichkeit zu übermittelnder personenbezogener Daten festzulegen und eine Auskunft über die Verwendung solcher Daten zu verlangen.

Der Anwendungsbereich der Vorschrift entspricht demjenigen des Artikels 27 Abs. 1. Die Erledigung eines Rechtshilfeersuchens kann die ersuchte Vertragspartei von zwei Bedingungen abhängig machen (vgl. Absatz 2): Sie kann erstens die Überlassung von Informationen oder Unterlagen an die Bedingung knüpfen, dass sie vertraulich behandelt werden, wenn dem Ersuchen ohne eine solche Bedingung nicht entsprochen werden könnte. Zweitens kann sie die Übermittlung von Informationen oder Unterlagen davon abhängig machen, dass diese nicht für andere als die im Ersuchen genannten Ermittlungen oder Verfahren verwendet werden. Hierauf muss sich die ersuchte Vertragspartei aber ausdrücklich berufen; andernfalls ist die Verwendung der übermittelten Informationen oder Unterlagen nicht beschränkt.

Die ersuchende Vertragspartei muss die ersuchte Vertragspartei darüber informieren, ob sie einer Bedingung nach Absatz 2 entsprechen kann. Ist dies nicht der Fall, steht es der ersuchten Vertragspartei frei, zu entscheiden, ob sie ihre Information dennoch zur Verfügung stellt. An die Annahme einer Bedingung ist die ersuchende Vertragspartei gebunden (Absatz 3). Die ersuchte Vertragspartei kann von der ersuchenden Vertragspartei Angaben über die Verwendung bedingt zur Verfügung gestellter Unterlagen oder Informationen verlangen (Absatz 4).

Abschnitt 2 – Besondere Bestimmungen

Zu Artikel 29 – Umgehende Sicherung gespeicherter Computerdaten

Dieser Artikel stellt das internationale Pendant zu der in Artikel 16 vorgesehenen beschleunigten Sicherung gespeicherter Computerdaten dar. Für ein solches Ersuchen um vorläufige Sicherung bedarf es keines förmlichen Rechtshilfeersuchens; vielmehr ist es ausreichend, dass das Ersuchen gewisse Anforderungen erfüllt, die in Absatz 2 dieser Vorschrift genannt sind. Zu diesen Anforderungen gehört neben bestimmten Angaben auch die Mitteilung der Absicht, ein auf Durchsuchung, Beschlagnahme oder Herausgabe der Daten gerichtetes Rechtshilfeersuchen nachzureichen. Artikel 29 bedarf keiner Umsetzung in deutsches Recht. Selbst im vertragslosen Bereich sieht das IRG eine umfassende Regelung in diesem Bereich vor. Nach § 67 Abs. 1 IRG kann bereits vor Eingang eines entsprechenden Ersuchens eine Beschlagnahme oder sonstige Sicherstellung vorgenommen werden, wenn die Herausgabe der sicherzustellenden Gegenstände an den ersuchenden Staat in Betracht kommt.

Da die beschleunigte Sicherung von Daten noch nicht deren Weitergabe an die ersuchende Vertragspartei impliziert, darf die ersuchte Vertragspartei nicht die beiderseitige Strafbarkeit zur Voraussetzung der Gewährung von Rechtshilfe machen (Verzicht auf den Einwand der beiderseitigen Strafbarkeit, vgl. Absatz 3). Nur wenn sie Grund zu der Annahme hat, dass im Zeitpunkt der Weitergabe die Voraussetzung der beiderseitigen Strafbarkeit nicht erfüllt werden kann, darf sie das Ersuchen unter Berufung auf die fehlende Strafbarkeit der dem Ersuchen zugrunde liegenden Handlung nach deutschem Recht ablehnen (Absatz 4). Dies gilt jedoch nicht für die in den Artikeln 2 bis 11 festgelegten Straftaten; das Vorliegen einer Strafbarkeit nach diesen Vorschriften wird vom Übereinkommen im Falle der Ratifizierung unterstellt und ist nach deutschem Recht gegeben (vgl. die Ausführungen zu den Artikeln 2 bis 11). Der Ablehnungsgrund gilt weiterhin nur, wenn eine Vertragspartei die beiderseitige Strafbarkeit als Voraussetzung für die Erledigung eines Rechtshilfeersuchens normiert hat. Das ist in Deutschland bei der Herausgabe von Gegenständen an ausländische Staaten nach § 66 Abs. 2 Nr. 1 IRG der Fall.

Daher wird erklärt, dass von Artikel 42 des Übereinkommens insoweit Gebrauch gemacht wird, als für die Ersuchen um umgehende Sicherung von Daten nach Artikel 29 der Ablehnungsgrund der beiderseitigen Strafbarkeit gilt, es sei denn, es handelt sich um eine nach den Artikeln 2 bis 11 umschriebene Straftat.

Zwei weitere Ablehnungsgründe, die abschließend sind und mit den in Artikel 27 Abs. 4 genannten übereinstimmen, enthält Absatz 5.

Die ersuchende Vertragspartei ist umgehend zu informieren, wenn durch die Sicherung nach Ansicht der ersuchten Vertragspartei die künftige Verfügbarkeit der Daten nicht gewährleistet oder die Vertraulichkeit der Ermittlungen der ersuchenden Vertragspartei gefährdet oder in anderer Weise beeinträchtigt ist (Absatz 6).

Die ersuchte Vertragspartei ist verpflichtet, sicherzustellen, dass die Datensicherung zunächst für mindestens sechzig Tage erfolgt beziehungsweise nach Eingang des förmlichen Rechtshilfeersuchens bis zur Entscheidung über dieses Ersuchen aufrechterhalten bleibt.

Zu Artikel 30 – Umgehende Weitergabe gesicherter Verkehrsdaten

Artikel 30 ist das Gegenstück zu Artikel 17 des Übereinkommens. Er betrifft den Fall, dass sich im Zuge der Erledigung eines Ersuchens nach Artikel 29 herausstellt, dass ein Diensteanbieter in einem anderen Staat an der Übertragung einer bestimmten Kommunikation beteiligt war. Die ersuchte Vertragspartei muss dann beschleunigt Verkehrsdaten in solchem Umfang weitergeben, dass der Diensteanbieter und der Übertragungsweg festgestellt werden können. Die Weitergabe darf nur aus den in Absatz 2 abschließend aufgezählten Gründen, die mit denen in Artikel 29 Abs. 5 inhaltlich übereinstimmen, abgelehnt werden. Da im deutschen Recht durch die beabsichtigte Neuregelung in § 100g StPO eine umfassende Erhebungsbefugnis für Verkehrsdaten besteht (vgl. Artikel 17), ist eine Weitergabe von Verkehrsdaten nach den für Deutschland geltenden multilateralen und bilateralen Vereinbarungen oder nach den §§ 59 ff. IRG möglich.

Zu Artikel 31 – Rechtshilfe beim Zugriff auf gespeicherte Computerdaten

Diese Vorschrift stellt das Pendant zu Artikel 19 des Übereinkommens dar. Nach Absatz 1 darf um diese Art von Rechtshilfe ersucht werden; nach Absatz 2 muss die ersuchte Vertragspartei nach den vorgesehenen Bedingungen in der Lage sein, diese zu gewährleisten. Absatz 3 regelt die Fälle, in denen ein Ersuchen beschleunigt zu erledigen ist. Umsetzungsbedarf besteht nicht. Sofern keine bi- oder multilateralen Vereinbarungen bestehen, ist im vertragslosen Verkehr die Gewährung der Rechtshilfe nach dem IRG möglich. Die Möglichkeit der Herausgabe von Gegenständen richtet sich nach § 66 IRG.

Zu Artikel 32 – Grenzüberschreitender Zugriff auf gespeicherte Computerdaten mit Zustimmung oder wenn diese öffentlich zugänglich sind

Diese Vorschrift regelt den einseitigen Zugriff einer Vertragspartei auf gespeicherte Daten auf dem Gebiet einer anderen Vertragspartei ohne Rechtshilfeersuchen. Buchstabe a bezieht sich auf den Zugriff auf öffentlich zugängliche gespeicherte Computerdaten. In Buchstabe b ist der Zugriff auf im Hoheitsgebiet eines anderen Staates gespeicherte, nichtöffentliche Daten geregelt, auf die eine bestimmte inländische Person Zugriff hat, die rechtmäßig befugt ist, die Daten an inländische Strafverfolgungsbehörden weiterzugeben, und ihre rechtmäßige und freiwillige Zustimmung zum grenzüberschreitenden Zugriff erteilt hat. Nur dieser grenzüberschreitende Zugriff auf gespeicherte Daten ist Regelungsgegenstand und soll erfolgen können, ohne dass ein an die Behörden des anderen Staates gerichtetes Rechtshilfeersuchen erforderlich wäre. Diese Vorschrift stellt keine Ausnahme zur formalisierten Rechtshilfe dar. Beide hoheitlichen Handlungen sind nach den innerstaatlichen strafprozessualen Vorschriften zulässig.

Zu den Artikeln 33 und 34 – Rechtshilfe bei der Erhebung von Verkehrs- und Inhaltsdaten in Echtzeit

Die beiden Rechtshilfevorschriften knüpfen an die Echtzeit-Erhebung von Verkehrsdaten (Artikel 20) und von Inhaltsdaten (Artikel 21) an.

Dem Grundsatz nach leisten die Vertragsparteien einander Rechtshilfe bei der Echtzeit-Erhebung von Verkehrsdaten. Diese unterliegt dabei den in den anwendbaren Verträgen, Vereinbarungen und Rechtsvorschriften enthaltenen Bestimmungen, wobei die Reihe der Straftaten, in denen in solchen Fällen Rechtshilfe gewährt wird, in keinem Fall enger gefasst sein darf als diejenige, die für eine solche Maßnahme in einem gleichartigen inländischen Fall zur Verfügung steht.

Im Falle der Echtzeit-Erhebung von Inhaltsdaten beschränkt sich die Verpflichtung zur Leistung von Rechtshilfe aufgrund des damit verbundenen erheblichen Eingriffs in die Privatsphäre dagegen auf das in anwendbaren Verträgen und innerstaatlichen Rechtsvorschriften zulässige Maß. Weitergehende Verpflichtungen legt das Übereinkommen nicht fest.

Maßstab für die Rechtshilfe in diesem Bereich ist daher nicht das Niveau des ersuchenden Staates, sondern das deutsche Recht. Dies ist insbesondere bei Rechtshilfeersuchen von Staaten mit niedrigeren datenschutzrechtlichen Strukturen von Bedeutung.

Zu Artikel 35 – 24/7-Netzwerk

Die Schaffung eines Netzwerks unter den Vertragsparteien, das rund um die Uhr besetzt ist, stellt eine wichtige Komponente bei der Bekämpfung der Computerkriminalität dar. Die flüchtige Welt der Daten erfordert oftmals eine schnelle Reaktion, die nur durch unverzügliche Unterstützung sichergestellt werden kann. Der Umfang dieser Unterstützung ergibt sich aus Absatz 1 Satz 2 und findet seine Grenze im innerstaatlichen Recht. Es ist nicht erforderlich, dass die nationale Kontaktstelle bei den für die Rechtshilfe nach Artikel 27 Abs. 2 oder für die Auslieferung nach Artikel 24 Abs. 7 zuständigen Stellen angesiedelt ist, solange eine schnelle Abstimmung mit diesen Behörden sichergestellt ist.

Kapitel IV
Schlussbestimmungen

Zu den Artikeln 36 bis 48

Diese Artikel enthalten im Wesentlichen die in Europarat-Übereinkommen verwendeten Schlussklauseln. Daher soll nur auf die wichtigsten Punkte eingegangen werden.

Nach Artikel 36 sind zur Unterzeichnung des Übereinkommens nur die Mitgliedstaaten des Europarats und die an der Ausarbeitung beteiligten Nichtmitgliedstaaten berechtigt. Andere Nichtmitgliedstaaten können dem Übereinkommen nach dessen Inkrafttreten allerdings auf Einladung des Ministerkomitees des Europarats beitreten (Artikel 37).

Wie bereits dargestellt, enthält Artikel 40 die Möglichkeit der Abgabe von Erklärungen und Artikel 42 die Möglichkeit der Einlegung von Vorbehalten.

Nach Artikel 43 Abs. 3 kann der Generalsekretär des Europarats sich in regelmäßigen Abständen bei den Vertragsparteien nach den Aussichten über die Rücknahme der eingelegten Vorbehalte erkundigen.

Die Regelung in Artikel 44 ist hauptsächlich für kleinere Änderungen des Verfahrens gedacht; bedeutendere Änderungen des Übereinkommens bedürfen der Form eines Zusatzprotokolls.

Streitigkeiten über die Auslegung oder Anwendung des Übereinkommens sollen gemäß Artikel 45 Abs. 2 zwischen den betroffenen Parteien friedlich beigelegt werden, möglichst durch Verhandlungen, andernfalls durch eine gegenseitige Vereinbarung, den Europäischen Ausschuss für Strafrechtsfragen, ein Schiedsgericht oder den Internationalen Gerichtshof mit der Streitfrage zu befassen und sich dessen Spruch zu unterwerfen.

In Artikel 46 ist die Konsultation der Vertragsparteien bei Bedarf in regelmäßigen Abständen geregelt, um eine wirksame Anwendung und Durchführung dieses Übereinkommens, den Informationsaustausch über wichtige Entwicklungen im Bereich der Computerkriminalität und um Überlegungen etwaiger Ergänzungen oder Änderungen des Übereinkommens zu erleichtern.

Anlage zur Denkschrift

Übereinkommen über Computerkriminalität (ETS Nr. 185)
Erläuternder Bericht
(am 8. November 2001 angenommen)

I. Das Übereinkommen und der Erläuternde Bericht sind vom Ministerkomitee des Europarats auf seiner 109. Tagung (8. November 2001) angenommen worden; das Übereinkommen wurde am 23. November 2001 in Budapest anlässlich der Internationalen Konferenz über Computerkriminalität zur Unterzeichnung aufgelegt.

II. Der Erläuternde Bericht stellt kein Instrument dar, das die Auslegung des Übereinkommens maßgeblich bestimmt, es kann jedoch dazu dienen, die Anwendung der Bestimmungen des Übereinkommens zu erleichtern.

I. Einleitung

1. Die revolutionäre Entwicklung im Bereich der Informationstechnik hat die Gesellschaft grundlegend verändert und dürfte dies in naher Zukunft wohl weiterhin tun. Viele Aufgaben sind dadurch erleichtert worden. Während zunächst nur bestimmte Bereiche der Gesellschaft ihre Arbeitsmethoden mit Hilfe der Informationstechnik rationalisiert haben, bleibt nunmehr kaum ein Bereich hiervon unberührt. Die Informationstechnik durchdringt in der einen oder anderen Form nahezu jeden Aspekt menschlicher Tätigkeit.

2. Ein auffallendes Merkmal der Informationstechnik ist ihre Auswirkung auf die Entwicklung der Telekommunikationstechnologie. Die herkömmliche Fernsprechtechnik im Sinne einer Übertragung der menschlichen Stimme ist von dem Austausch riesiger Datenmengen eingeholt worden, die aus Stimme, Text, Musik, statischen oder beweglichen Bildern bestehen können. Dieser Austausch erfolgt nicht nur zwischen Menschen, sondern auch zwischen Menschen und Computern und zwischen Computern. Durchschalteverbindungen sind durch Netzwerke mit Datenpaketvermittlung ersetzt worden. Unerheblich ist demnach, ob eine Direktschaltung eingerichtet werden kann: Es reicht aus, dass Daten in ein Netzwerk mit einer Zieladresse eingegeben oder für alle bereitgestellt werden, die auf sie zugreifen möchten.

3. Die weit verbreitete Nutzung der elektronischen Post und der Zugang zu zahlreichen Websites über das Internet sind Beispiele dieser Entwicklungen, die unsere Gesellschaft tiefgreifend verändert haben.

4. Die Tatsache, dass man bequem auf die in Computersystemen enthaltenen Informationen zugreifen und diese abrufen kann, hat zusammen mit den praktisch unbegrenzten Möglichkeiten des Austauschs und der Verbreitung dieser Informationen ungeachtet geographischer Entfernungen zu einem explosionsartigen Anstieg der verfügbaren Informationsmenge und des daraus zu ziehenden Wissens geführt.

5. Diese Entwicklung hat zu einem beispiellosen ökonomischen und sozialen Wandel geführt, weist aber auch Schattenseiten auf: das Entstehen neuer Formen der Kriminalität und die Begehung herkömmlicher Delikte mit Hilfe der neuen Technologien. Außerdem können die Auswirkungen des kriminellen Handelns weitreichender als früher sein, weil sie weder durch geographische Begrenzungen noch durch Staatsgrenzen beschränkt werden. Die jüngste Verbreitung von schädlichen Computerviren weltweit stellt diese Tatsache klar unter Beweis. Es müssen technische Maßnahmen zum Schutz von Computersystemen und gleichzeitig rechtliche Maßnahmen zur Verhütung der Kriminalität und zur Abschreckung ergriffen werden.

6. Die neuen Technologien stellen die vorhandenen Rechtsgrundsätze in Frage. Der Fluss von Informationen und Kommunikationen ist weltweit einfacher geworden. Grenzen bilden hierbei keine Hindernisse mehr. Mehr und mehr befinden sich Straftäter weit entfernt von den Orten, an denen ihre Handlungen Wirkung zeigen. Jedoch sind die innerstaatlichen Rechtsvorschriften gewöhnlich auf ein bestimmtes Hoheitsgebiet beschränkt. Die Antworten auf die gestellten Fragen müssen daher im Völkerrecht gesucht werden, was die Annahme geeigneter internationaler Rechtsinstrumente voraussetzt. Ziel dieses Übereinkommens ist es, dieser Herausforderung unter Achtung der Menschenrechte in der neuen Informationsgesellschaft zu begegnen.

II. Die vorbereitenden Arbeiten

7. Der Lenkungsausschuss für Strafrechtsfragen (CDPC) hat mit seiner Entscheidung CDPC/103/211196 im November 1996 beschlossen, einen Sachverständigenausschuss für Computerkriminalität zu schaffen. Der CDPC begründete seine Entscheidung wie folgt:

8. „Die rasanten Fortschritte im Bereich der Informationstechnologie wirken sich unmittelbar auf alle Bereiche unserer Gesellschaft aus. Die Einbeziehung von Telekommunikations- und Informationssystemen, die eine entfernungsunabhängige Speicherung und Übertragung von Daten aller Art gestatten, bieten ein breites Spektrum neuer Möglichkeiten. Gefördert wurden diese Entwicklungen durch das Entstehen von Netzwerken und Datenautobahnen, insbesondere durch das Internet, über die nahezu jedermann Zugriff auf die gesamten elektronischen Informationen überall in der Welt nehmen kann. Durch die Anbindung an die Kommunikations- und Informationsdienste schaffen die Nutzer eine Art gemeinsamen virtuellen Raum, den sogenannten Cyberspace, der rechtmäßigen Zwecken dient, aber auch dem Missbrauch offen steht. Diese im Cyberspace begangenen Straftaten richten sich gegen die Integrität, die Verfügbarkeit und die Vertraulichkeit von Computersystemen und Telekommunikationsnetzwerken oder bestehen aus der Nutzung dieser Netzwerke und Dienste zwecks Begehung herkömmlicher Straftaten. Die grenzüberschreitende Struktur dieser Straftaten – z. B. der über das Internet verübten Straftaten – steht im Widerspruch zur Territorialität der innerstaatlichen Strafverfolgungsbehörden.

9. Das Strafrecht muss daher mit diesen technischen Entwicklungen Schritt halten, die äußerst ausgefeilte Möglichkeiten zum Missbrauch des Cyberspace und zur Beeinträchtigung rechtmäßiger Interessen bieten. Da Informationsnetzwerke grenzüberschreitend sind, bedarf es abgestimmter internationaler Bemühungen, um solchem Missbrauch zu begegnen. Die Empfehlung Nr. R (89) 9 hat zwar dazu beigetragen, die innerstaatlichen Konzepte in Bezug auf bestimmte Formen der missbräuchlichen Computernutzung anzugleichen, aber einzig ein verbindliches internationales Rechtsinstrument dürfte die erforderliche Wirksamkeit bei der Bekämpfung dieser neuartigen Phänomene sicherstellen. Ein solches Instrument sollte nicht nur Maßnahmen der internationalen Zusammenarbeit vorsehen, sondern auch Fragen des materiellen Rechts sowie des Verfahrensrechts behandeln und ebenso Bereiche umfassen, die eng mit der Nutzung der Informationstechnik verknüpft sind."

10. Darüber hinaus hat der CDPC den auf seine Bitte von Professor H.W.K. Kaspersen erstellten Bericht berücksichtigt, in dem es abschließend heißt: "... man sollte sich auf ein anderes Rechtsinstrument berufen, das verbindlicher als eine Empfehlung ist, wie beispielsweise ein Übereinkommen. Ein solches Übereinkommen sollte nicht nur Fragen des materiellen Strafrechts angehen, sondern auch strafverfahrensrechtliche Aspekte beleuchten wie auch internationale strafrechtliche Verfahren und Vereinbarungen."[1]) Eine ähnliche Schlussfolgerung weist der Bericht zu der Empfehlung Nr. R (89) 9[2]) bezüglich des materiellen Rechts und die Empfehlung Nr. R (95) 13[3]) über die strafverfahrensrechtlichen Probleme im Zusammenhang mit der Informationstechnologie auf.

11. Dem neuen Ausschuss wurde das folgende Mandat erteilt:

i. „Im Licht der Empfehlung Nr. R (89) 9 über computerbezogene Straftaten und der Empfehlung Nr. R (95) 13 über die strafverfahrensrechtlichen Probleme im Zusammenhang mit der Informationstechnologie sollen insbesondere folgende Fragen behandelt werden:

ii. Die Computerstraftaten unter besonderer Berücksichtigung derjenigen, die unter Einsatz von Telekommunikationsnetzwerken, z. B. dem Internet, begangen werden, wie rechtswidrige Geldgeschäfte, Anbieten von rechtswidrigen Dienstleistungen, Verstöße gegen das Urheberrecht sowie Handlungen, welche die Menschenwürde und den Schutz von Minderjährigen verletzen;

iii. sonstige Fragen des materiellen Strafrechts, die zum Zwecke der internationalen Zusammenarbeit einer gemeinsamen Basis bedürfen, wie die Begriffsbestimmungen, die Sanktionen und die Verantwortlichkeit der im Cyberspace Handelnden einschließlich der Internet-Diensteanbieter;

iv. Einsatz von Zwangsmaßnahmen – einschließlich der Möglichkeit des grenzüberschreitenden Einsatzes – und Anwendbarkeit von Zwangsmaßnahmen im technologischen Umfeld, z. B. Abfangen von Telekommunikationen und elektronische Überwachung von Informationsnetzwerken (über das Internet u. Ä.), Durchsuchung und Beschlagnahme in Datenverarbeitungssystemen (einschließlich der Internet-Seiten), Maßnahmen, um das rechtswidrige Material unzugänglich zu machen, und Verpflichtung der Diensteanbieter zur Einhaltung besonderer Auflagen, wobei die von bestimmten Maßnahmen zur Informationssicherung verursachten Probleme zu berücksichtigen sind (z. B. Verschlüsselung);

v. die Frage der Zuständigkeit bei der Datennetzkriminalität, z. B. Bestimmung des Handlungsortes *(locus delicti)* und des in der Sache anwendbaren Rechts einschließlich des Problems des *ne bis idem* im Falle mehrfacher Zuständigkeit und die Frage der Lösung positiver und der Vermeidung negativer Zuständigkeitskonflikte;

vi. Fragen der internationalen Zusammenarbeit bei der Ermittlung von Computerstraftaten in enger Zusammenarbeit mit dem Sachverständigenausschuss für die Anwendung europäischer Übereinkommen auf dem Gebiet des Strafrechts (PC-OC).

Der Ausschuss soll ein verbindliches Rechtsinstrument erarbeiten, das sich so weit wie möglich auf die Punkte i) bis v) stützt, wobei insbesondere die internationalen Aspekte und gegebenenfalls zusätzliche Empfehlungen zu bestimmten Bereichen hervorgehoben werden sollten. Der Ausschuss kann Vorschläge zu weiteren Punkten im Licht der technologischen Entwicklungen unterbreiten."

12. Im Anschluss an die Entscheidung des CDPC hat das Ministerkomitee mit seiner auf der 583. Tagung der Ministerdelegierten (am 4. Februar 1997) angenommenen Entscheidung Nr. CM/Del/Dec(97)583 den neuen Ausschuss mit der Bezeichnung „Sachverständigenausschuss für Datennetzkriminalität (PC-CY)" eingesetzt. Der PC-CY nahm seine Tätigkeit im April 1997 auf und begann die Verhandlungen über den Entwurf eines internationalen Übereinkommens über Computerkriminalität. Nach dem ursprünglichen Mandat sollte der Ausschuss seine Arbeiten am 31. Dezember 1999 beenden. Da er zu dem Zeitpunkt jedoch nicht in der Lage war, die Erörterungen zu bestimmten Punkten des Übereinkommens abzuschließen, wurde sein Mandat mit der Entscheidung Nr. CM/Del/Dec(99)679 der Ministerdelegierten bis zum 31. Dezember 2000 verlängert. Die europäischen Justizminister haben zweimal ihre Unterstützung des Planes bekräftigt: einmal mit der bei ihrer 21. Konferenz (Prag, Juni 1997) angenommenen Entschließung Nr. 1, mit der dem Ministerkomitee empfohlen wurde, die Tätigkeit des Lenkungsausschusses für Strafrechtsfragen (CDPC) zur Computerkriminalität zu unterstützen, um die innerstaatlichen Strafrechtsbestimmungen zu harmonisieren und wirksame Verfahren zur Ermittlung solcher Straftaten zu ermöglichen, und zum anderen mit der bei der 23. Konferenz der europäischen Justizminister (London, Juni 2000) angenommenen Entschließung Nr. 3, mit der die Verhandlungspartner zur Fortführung ihrer Bemühungen angeregt wurden, um geeignete Lösungen zu finden und somit einer größtmöglichen Zahl an Staaten zu gestatten, dem Übereinkommen als Vertragspartei beizutreten, und mit der das Erfordernis anerkannt wurde, über einen raschen und wirksamen Mechanismus der internationalen Zusammenarbeit unter gebührender Berücksichtigung der besonderen Erfordernisse bei der Bekämpfung der Computerkriminalität zu verfügen. Die Mitgliedstaaten der Europäischen Union haben in einer im Mai 1999 angenommenen gemeinsamen Erklärung ihre Unterstützung der Arbeit des PC-CY zum Ausdruck gebracht.

13. Zwischen April 1997 und Dezember 2000 hat der PC-CY 10 Plenarsitzungen und 15 Sitzungen seines zeitlich nicht begrenzten Redaktionsausschusses abgehalten. Nach Ablauf der Verlängerung seines Mandats haben die Sachverständigen unter Federführung des CDPC drei weitere Sitzungen abgehalten, um den Entwurf des Erläuternden Berichts abzuschließen und den Übereinkommensentwurf im Licht der Stellungnahme der Parlamentarischen Versammlung zu prüfen. Die Versammlung wurde im Oktober 2000 vom Ministerkomitee gebeten, eine Stellungnahme zu dem Übereinkommensentwurf abzugeben, die sie im zweiten Teil ihrer Vollversammlung im April 2001 angenommen hat.

14. Nach einer Entscheidung des PC-CY wurde eine frühe Fassung des Übereinkommensentwurfs im April 2000 freigegeben, gefolgt von späteren, nach jeder Plenarsitzung freigegebenen Entwürfen, um es den verhandelnden Staaten zu ermöglichen, alle interessierten Stellen zu konsultieren. Dieses Konsultationsverfahren hat sich als nützlich erwiesen.

15. Die revidierte und endgültige Fassung des Übereinkommensentwurfs und des Erläuternden Berichts hierzu ist dem CDPC bei seiner 50. Plenarsitzung im Juni 2001 zur Genehmigung vorgelegt worden, woraufhin der Wortlaut des Übereinkommensentwurfs dem Ministerkomitee zur Annahme und Auflegung zur Unterzeichnung unterbreitet wurde.

III. Das Übereinkommen

16. Das Übereinkommen zielt hauptsächlich darauf ab, (1) die Tatbestandsmerkmale im innerstaatlichen materiellen Strafrecht sowie verwandte Bestimmungen auf dem Gebiet der Computerkriminalität zu harmonisieren, (2) im innerstaatlichen Strafverfahrensrecht die Befugnisse vorzusehen, die zur Ermittlung und Verfolgung solcher Straftaten und anderer mit Hilfe eines Computersystems begangener Straftaten notwendig sind oder zu denen Beweise in elektronischer Form vorliegen und (3) ein schnelles und wirksames System der internationalen Zusammenarbeit zu errichten.

17. Das Übereinkommen ist dementsprechend in vier Kapitel gegliedert: I) Begriffsbestimmungen; II) Innerstaatlich zu treffende Maßnahmen – Materielles Strafrecht und Verfahrensrecht; III) Internationale Zusammenarbeit und IV) Schlussbestimmungen.

18. Kapitel II Abschnitt 1 (Materielles Strafrecht) behandelt Bestimmungen zur Kriminalisierung wie auch andere verwandte Bestimmungen auf dem Gebiet der Computerkriminalität: Zunächst werden neun Straftaten in vier unterschiedlichen Kategorien umschrieben, sodann werden weitere Formen der Verantwortlichkeit und Sanktionen behandelt. Das Übereinkommen definiert folgende Straftaten: rechtswidriger Zugang, rechtswidriges Abfangen, Eingriff in Daten, Eingriff in ein System, Missbrauch von Vorrichtungen, Computerbezogene Fälschung, Computerbezogener Betrug, Straftaten mit Bezug zu Kinderpornografie und Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte.

19. Kapitel II Abschnitt 2 (Fragen des Verfahrensrechts) – dessen Geltungsbereich über die Straftaten nach Abschnitt 1 hinausgeht, weil er sich auf alle mittels eines Computersystems begangene Straftaten oder auf solche bezieht, zu denen Beweise in elektronischer Form vorliegen – legt zunächst die gemeinsamen Bedingungen und Garantien fest, die auf alle in diesem Kapitel bezeichneten verfahrensrechtlichen Befugnisse anwendbar sind. Es werden folgende Befugnisse und Verfahren aufgeführt: umgehende Sicherung gespeicherter Computerdaten, umgehende Sicherung und teilweise Weitergabe von Verkehrsdaten, Anordnung der Herausgabe, Durchsuchung und Beschlagnahme gespeicherter Computerdaten, Erhebung von Verkehrsdaten in Echtzeit und Abfangen von Inhaltsdaten in Echtzeit. Kapitel II schließt mit den Bestimmungen über Gerichtsbarkeit ab.

20. Kapitel III regelt die Rechtshilfe bei herkömmlichen und computerbezogenen Straftaten sowie Fragen der Auslieferung. Die klassische Rechtshilfe tritt in zwei Fällen auf: Zwischen den Vertragsparteien besteht entweder keine rechtliche Grundlage (Vertrag, gegenseitige Rechtsvorschriften usw.) – wobei die Bestimmungen dieses Kapitels anwendbar sind – oder eine rechtliche Grundlage ist gegeben, wobei die bestehenden Regelungen auch für die Rechtshilfe nach diesem Übereinkommen gelten. Die Rechtshilfe in Bezug auf die Computerkriminalität ist auf beide Fälle anwendbar und erstreckt sich – vorbehaltlich zusätzlicher Bedingungen – auf denselben Katalog von Verfahrensbefugnissen entsprechend Kapitel II. Darüber hinaus enthält Kapitel III eine Bestimmung über eine besondere Form des grenzüberschreitenden Zugriffs auf gespeicherte Daten, die keiner Rechtshilfe bedarf („mit Zustimmung oder wenn diese öffentlich zugänglich sind“), und sieht die Schaffung eines 24/7-Netzwerks für die schnelle Rechtshilfe zwischen den Vertragsparteien vor.

21. Kapitel IV enthält schließlich die Schlussbestimmungen, die sich bis auf wenige Ausnahmen an die Standardvertragsklauseln des Europarats anlehnen.

Bemerkungen zu den Artikeln des Übereinkommens

Kapitel I Begriffsbestimmungen

Einleitung zu den Begriffsbestimmungen in Artikel 1

22. Die Verfasser gingen davon aus, dass die Vertragsparteien dieses Übereinkommens nicht verpflichtet sind, die vier in Artikel 1 definierten Konzepte wörtlich in ihr innerstaatliches Recht zu übernehmen, vorausgesetzt, dieses Recht erfasst diese Konzepte in einer den Grundsätzen des Übereinkommens entsprechenden Weise und bietet einen gleichwertigen Rahmen für ihre Durchsetzung.

Artikel 1 Buchstabe a – Computersystem

23. Ein Computersystem im Sinne des Übereinkommens ist eine aus Hardware und Software bestehende Vorrichtung, die zur automatischen Verarbeitung digitaler Daten entwickelt wurde. Sie kann Eingabe-, Ausgabe- und Speichereinheiten enthalten. Sie kann einzeln vorhanden sein oder in einem Netzwerk mit anderen ähnlichen Vorrichtungen verbunden sein. „Automatisch“ bedeutet ohne unmittelbares menschliches Eingreifen, „Datenverarbeitung“ bedeutet, dass Daten in einem Computersystem durch Ausführung eines Computerprogramms bearbeitet werden. Ein „Computerprogramm“

ist ein Satz Anweisungen, die vom Computer zur Erzielung des beabsichtigten Ergebnisses ausgeführt werden. Ein Computer kann verschiedene Programme ausführen. Ein Computersystem besteht gewöhnlich aus verschiedenen Vorrichtungen, bei denen zwischen dem Rechner oder der Zentraleinheit und peripheren Einheiten unterschieden wird. Eine „periphere Einheit“ ist eine Vorrichtung, die bestimmte besondere Funktionen in Interaktion mit der zentralen Einheit durchführt, wie ein Drucker, Bildschirm, CD-Reader/Writer oder eine andere Speichervorrichtung.

24. Ein Netzwerk ist ein Verbund zwischen zwei oder mehr Computersystemen. Die Verbindungen können erdgebunden (z. B. Draht oder Kabel), drahtlos (z. B. Funk, Infrarot oder Satellit) oder beides sein. Ein Netzwerk kann geographisch auf ein kleines Gebiet begrenzt sein (Lokalnetze) oder sich über ein großes Gebiet erstrecken (Breitnetz) und derartige Netzwerke können selbst einen Verbund darstellen. Das Internet ist ein globales Netzwerk, das aus vielen verbundenen Netzwerken besteht, die alle dieselben Protokolle verwenden. Es gibt auch andere Arten von Netzwerken, ob mit dem Internet verbunden oder nicht, die Computerdaten zwischen Computersystemen übermitteln können. Computersysteme können mit dem Netzwerk als Endpunkte oder als Mittel zur Unterstützung der Kommunikation im Netzwerk verbunden sein. Wesentlich ist, dass über das Netzwerk Daten ausgetauscht werden.

Artikel 1 Buchstabe b – Computerdaten

25. Die Definition von Computerdaten basiert auf der ISO-Definition von Daten. Diese Definition enthält den Ausdruck „für die Verarbeitung geeignet“. Das bedeutet, dass Daten in eine Form gebracht werden, in der sie unmittelbar vom Computersystem verarbeitet werden können. Um deutlich zu machen, dass unter Daten in diesem Übereinkommen Daten in elektronischer oder sonstiger unmittelbar verarbeitbarer Form zu verstehen sind, wird der Begriff „Computerdaten“ eingeführt. Computerdaten, die automatisch verarbeitet werden, können Ziel einer der in diesem Übereinkommen umschriebenen Straftaten sowie Gegenstand der Anwendung einer der in diesem Übereinkommen umschriebenen Ermittlungsmaßnahmen sein.

Artikel 1 Buchstabe c – Diensteanbieter

26. Der Begriff „Diensteanbieter“ umfasst eine große Gruppe von Personen, die eine besondere Rolle bei der Kommunikation und Verarbeitung von Daten in Computersystemen spielen (vgl. auch Bemerkungen zu Abschnitt 2). In Ziffer i der Begriffsbestimmung wird deutlich gemacht, dass sowohl öffentliche als auch private Organisationen, die es Nutzern ermöglichen, miteinander zu kommunizieren, erfasst sind. Daher ist es unerheblich, ob die Nutzer eine geschlossene Gruppe bilden oder ob der Anbieter seine Dienste der Öffentlichkeit anbietet, sei es kostenlos oder gegen Gebühr. Die geschlossene Gruppe kann z. B. aus den Angestellten eines privaten Unternehmens bestehen, denen der Dienst von einem Unternehmensnetz angeboten wird.

27. In Ziffer ii der Begriffsbestimmung wird deutlich gemacht, dass der Begriff „Diensteanbieter“ auch diejenigen Organisationen erfasst, die für die in Ziffer i genannten Personen Daten speichern oder auf andere Weise verarbeiten. Ferner schließt dieser Begriff auch diejenigen Organisationen ein, die für die Nutzer der Dienste der in Ziffer i genannten Organisationen Daten speichern oder auf andere Weise verarbeiten. Zum Beispiel umfasst nach dieser Definition ein Diensteanbieter sowohl Dienste in Form von *hosting and caching services* als auch Dienste, die eine Verbindung zu einem Netzwerk herstellen. Hingegen soll ein reiner Inhaltsanbieter (z. B. eine Person, die eine *web hosting company* beauftragt, ihre Website zu führen, nicht von dieser Definition erfasst werden, wenn dieser Inhaltsanbieter nicht auch Kommunikations- oder damit zusammenhängende Datenverarbeitungsdienste anbietet.

Artikel 1 Buchstabe d – Verkehrsdaten

28. Für die Zwecke dieses Übereinkommens stellen Verkehrsdaten in der Definition nach Artikel 1 Buchstabe d eine Gruppe von Computerdaten dar, die einer besonderen Regelung unterliegen. Diese Daten werden von Computern in der Kommunikationskette erzeugt, um eine Kommunikation von ihrem Ursprung zu ihrem Ziel zu leiten. Sie sind daher ein Hilfsmittel für die Kommunikation selbst.

29. Bei Ermittlungen wegen einer Straftat, die im Zusammenhang mit einem Computersystem begangen wurde, werden Verkehrsdaten benötigt, um die Quelle einer Kommunikation als Ausgangspunkt für die weitere Beweiserhebung oder als Teil der Beweise für eine Straftat aufzuspüren. Verkehrsdaten können kurzlebig sein, so dass es notwendig ist, ihre beschleunigte Sicherung anzuordnen. Ihre schnelle Weitergabe kann daher notwendig sein, damit der Leitweg der Kommunikation erkennbar wird, um weitere Beweise erheben zu können, bevor die Daten gelöscht werden, oder um einen Verdächtigen identifizieren zu können. Das normale Verfahren zur Erhebung und Weitergabe von Computerdaten könnte daher unzureichend sein. Außerdem wird die Erhebung dieser Daten grundsätzlich als weniger eingreifend angesehen, da sie als solche nicht den Inhalt der Kommunikation offenbart, der als vertraulicher gilt.

30. Die Begriffsbestimmung führt sämtliche Kategorien von Verkehrsdaten auf, die einer besonderen Regelung in diesem Übereinkommen unterliegen: Ursprung, Ziel, Leitweg, Uhrzeit, Datum, Umfang und Dauer einer Kommunikation und die Art des benutzten Dienstes. Nicht alle diese Kategorien werden immer technisch verfügbar sein oder von einem Diensteanbieter herausgegeben werden können oder für bestimmte strafrechtliche Ermittlungen notwendig sein. Der „Ursprung“ bezieht sich auf eine Telefonnummer, eine Internetprotokolladresse oder eine ähnliche Angabe zu einer Kommunikationsstelle, die von einem Diensteanbieter bedient wird. Das „Ziel“ bezieht sich auf eine vergleichbare Angabe zu einer Kommunikationsstelle, an die Kommunikationen übermittelt werden. Der Ausdruck „Art des Trägerdienstes“ bezieht sich auf die Art des Dienstes, der in einem Netz benutzt wird, z. B. Dateiübertragung („file transfer“), elektronische Post oder sofortige Mitteilungsübermittlung („instant messaging“).

31. Die Begriffsbestimmung überlässt es den nationalen Gesetzgebern, den gesetzlichen Schutz von Verkehrsdaten entsprechend ihrer Vertraulichkeit zu differenzieren. In diesem Zusammenhang verpflichtet Artikel 15 die Vertragsparteien, hinreichende Bedingungen und Garantien zum Schutz der Menschenrechte und Grundfreiheiten vorzusehen. Dies bedeutet unter anderem, dass die

materiellen Kriterien und das Verfahren zur Anwendung einer Ermittlungsbefugnis je nach Vertraulichkeit der Daten unterschiedlich sein können.

Kapitel II
Maßnahmen auf nationaler Ebene

32. Kapitel II (Artikel 2 – 22) enthält drei Abschnitte: materielles Strafrecht (Artikel 2 – 13), Verfahrensrecht (Artikel 14 – 21) und Gerichtsbarkeit (Artikel 22).

Abschnitt 1 – Materielles Strafrecht

33. Abschnitt 1 des Übereinkommens (Artikel 2 – 13) zielt auf die Verbesserung der Mittel zur Verhütung und Bekämpfung der Computerkriminalität durch die Schaffung eines einheitlichen Mindeststandards einschlägiger Straftatbestände. Diese Art der Harmonisierung erleichtert die Bekämpfung dieser Kriminalität auf nationaler wie auch auf internationaler Ebene. Die Übereinstimmung des innerstaatlichen Rechts kann die Verlagerung des Missbrauchs in das Gebiet einer Vertragspartei mit einem zuvor niedrigeren Standard verhindern. Dadurch kann auch der Austausch nützlicher allgemeiner Erfahrungen im praktischen Umgang mit derartigen Fällen gefördert werden. Die internationale Zusammenarbeit (insbesondere Auslieferung und Rechtshilfe) wird z. B. hinsichtlich der Anforderungen der beiderseitigen Strafbarkeit erleichtert.

34. Die Liste der Straftaten stellt einen Mindestkonsens dar und schließt Ergänzungen im innerstaatlichen Recht nicht aus. Sie basiert im Wesentlichen auf den im Zusammenhang mit der Europaratsempfehlung Nr. R (89) 9 über computerbezogene Straftaten entwickelten Leitlinien und auf der Arbeit anderer öffentlicher und privater internationaler Organisationen (OECD, VN, AIDP), berücksichtigt aber auch neuere Erfahrungen mit dem Missbrauch der expandierenden Telekommunikation.

35. Der Abschnitt ist in fünf Titel unterteilt. Titel 1 behandelt den Kern der Computerstraftaten, Straftaten gegen die Vertraulichkeit, die Integrität und die Verfügbarkeit von Computerdaten und Computersystemen, die die grundlegenden Gefahren für elektronische Datenverarbeitungs- und Datenübermittlungssysteme darstellen, wie sie in den Diskussionen über Computer- und Datensicherheit geschildert werden. Die Überschrift bezeichnet die Art der jeweils erfassten Straftaten, d. h. unbefugter Zugriff auf Systeme, Programme oder Daten und deren rechtswidrige Veränderung. Die Titel 2 bis 4 behandeln andere Arten von Computerstraftaten, die in der Praxis eine größere Rolle spielen und bei denen Computer- und Telekommunikationssysteme dazu verwendet werden, bestimmte Rechtsgüter anzugreifen, die zumeist bereits durch das Strafrecht vor Angriffen mit traditionellen Mitteln geschützt sind. Die Straftaten in Titel 2 (Computerbezogener Betrug und Fälschung) wurden in Anlehnung an die Leitlinien der Europaratsempfehlung Nr. R (89) 9 eingefügt. Titel 3 behandelt die inhaltsbezogene Straftat der rechtswidrigen Herstellung und Verbreitung von Kinderpornografie mittels Computersystemen als eine der gefährlichsten Straftaten in jüngster Zeit. Der mit der Ausarbeitung des Übereinkommens befasste Ausschuss erörterte die mögliche Einbeziehung anderer inhaltsbezogener Straftaten wie die Verbreitung rassistischer Propaganda mittels Computersystemen. Der Ausschuss konnte jedoch keine Einigkeit über die Kriminalisierung solchen Verhaltens erzielen. Es gab zwar erhebliche Unterstützung für die Einbeziehung als Straftat, jedoch äußerten einige Delegationen starke Bedenken gegen das Einfügen einer solchen Bestimmung aus Gründen der Meinungsfreiheit. Angesichts der Komplexität dieser Frage wurde beschlossen, dass der Ausschuss die Frage der Ausarbeitung eines Zusatzprotokolls zum Übereinkommen der an den Lenkungsausschuss für Strafrechtsfragen (CDPC) verweisen soll. Titel 4 behandelt Straftaten, die sich auf die Verletzung des Urheberrechts und verwandter Schutzrechte beziehen. Dies wurde einbezogen, da Urheberrechtsverletzungen zu den verbreitetsten Formen der Computerkriminalität gehören und ihre Ausbreitung international Besorgnis erregt. Titel 5 schließlich enthält ergänzende Bestimmungen über den Versuch, die Beteiligung, Sanktionen und Maßnahmen sowie, entsprechend neueren internationalen Übereinkünften, über die Verantwortlichkeit juristischer Personen.

36. Obgleich sich die materiell-rechtlichen Bestimmungen auf Straftaten beziehen, die sich der Informationstechnik bedienen, verwendet das Übereinkommen eine technologie-neutrale Sprache, damit die materiell-rechtlichen Straftatbestände für derzeitige wie auch für künftige Technologien gelten.

37. Die Verfasser des Übereinkommens gingen davon aus, dass die Vertragsparteien geringfügige und unbedeutende Verstöße von der Anwendung der Straftatbestände nach Artikel 2 bis 10 ausschließen können.

38. Eine Besonderheit der einbezogenen Straftaten ist die ausdrückliche Voraussetzung, dass die betreffende Handlung „unbefugt“ begangen worden sein muss. Hier kommt die Erkenntnis zum Ausdruck, dass die beschriebene Handlung nicht immer an sich strafbar ist, sondern erlaubt oder gerechtfertigt sein kann, und zwar nicht nur in Fällen, in denen die klassischen Rechtfertigungsgründe wie Einwilligung, Notwehr oder Notstand gelten, sondern auch wenn andere Grundsätze oder Interessen zum Ausschluss der strafrechtlichen Verantwortlichkeit führen. Der Ausdruck „unbefugt“ erhält seine Bedeutung aus dem Zusammenhang, in dem er verwendet wird. Ohne vorzuschreiben, wie die Vertragsparteien dieses Konzept in ihr innerstaatliches Recht umsetzen, kann er sich auf Handlungen beziehen, die ohne (gesetzlich, exekutiv, administrativ, gerichtlich, vertraglich oder einvernehmlich erteilte) Befugnis erfolgen, oder auf Handlungen, die auch sonst nicht durch allgemein gültige Verteidigungsvorbringen, Befreiungen, Rechtfertigungsgründe oder diesbezügliche Grundsätze nach innerstaatlichem Recht abgedeckt sind. Das Übereinkommen lässt somit Handlungen unberührt, die aufgrund rechtmäßiger Staatsgewalt erfolgen (wenn z. B. die Regierung einer Vertragspartei zur Aufrechterhaltung der öffentlichen Ordnung, zum Schutz der nationalen Sicherheit oder zur Aufklärung von Straftaten handelt). Außerdem sollen rechtmäßige und gängige, sich aus der Netzwerkgestaltung ergebende Tätigkeiten oder rechtmäßige und gängige Betreiber- oder Unternehmenspraktiken nicht kriminalisiert werden. Einzelne Beispiele für derartige Ausnahmen von der Kriminalisierung werden zu den einzelnen Straftaten an der jeweiligen Stelle im Erläuternden Bericht angeführt. Es bleibt den Vertragsparteien überlassen festzulegen, wie diese Ausnahmen in ihrem innerstaatlichen Rechtssystem berücksichtigt werden (im Strafrecht oder auf andere Weise).

39. Alle im Übereinkommen erfassten Straftaten müssen „vorsätzlich“ begangen werden, damit die strafrechtliche Verantwortlichkeit gegeben ist. In einigen Fällen bildet ein zusätzliches subjektives Element ein Tatbestandsmerkmal. Zum Beispiel ist in Artikel 8 zu Computerbetrug die Absicht, einen wirtschaftlichen Vorteil zu erlangen, ein Tatbestandsmerkmal. Die Verfasser des Übereinkommens waren sich einig, dass die genaue Bedeutung von „vorsätzlich“ Sache der nationalen Auslegung sein soll.

40. Einige Artikel in diesem Abschnitt können bei der Umsetzung in innerstaatliches Recht durch näher beschriebene Voraussetzungen ergänzt werden. In anderen Fällen ist sogar die Möglichkeit eines Vorbehalts vorgesehen (vgl. Artikel 40 und 42). Diese unterschiedlichen Möglichkeiten eines restriktiveren Ansatzes bei der Kriminalisierung spiegeln die unterschiedliche Einschätzung der Gefährlichkeit eines bestimmten Verhaltens oder der Notwendigkeit strafrechtlicher Gegenmaßnahmen wider. Dadurch wird es den Regierungen und Parlamenten ermöglicht, ihre Kriminalpolitik in diesem Bereich flexibel zu gestalten.

41. Gesetze, in denen diese Straftaten festgelegt werden, sollen möglichst klar und eindeutig abgefasst werden, damit hinreichend vorhersehbar wird, welche Art von Handlungen strafrechtliche Sanktionen auslösen.

42. Im Lauf der Redaktionsarbeit prüften die Verfasser, ob es ratsam ist, noch andere als die in den Artikeln 2 bis 11 definierten Handlungen unter Strafe zu stellen, darunter das so genannte *cyber-squatting,* d. h. das Registrieren eines Domänenamens, der mit dem Namen einer bereits bestehenden und gewöhnlich recht bekannten Organisation oder mit dem Handelsnamen oder der Marke eines Produkts oder eines Unternehmens identisch ist. *Cyber-squatters* haben nicht die Absicht, den Domänenamen aktiv zu nutzen, und versuchen, dadurch einen finanziellen Vorteil zu erlangen, dass sie die betreffende Organisation – wenn auch indirekt – zwingen, für die Übertragung des Eigentums an den Domänenamen zu zahlen. Derzeit wird dieses Verhalten als eine markenrechtliche Frage betrachtet. Da Markenverletzungen nicht Gegenstand dieses Übereinkommens sind, hielten es die Verfasser nicht für angebracht, die Frage der Kriminalisierung solchen Verhaltens zu behandeln.

Titel 1
Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen

43. Die in den Artikeln 2 bis 6 beschriebenen Straftatbestände sind dazu bestimmt, die Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen und Computerdaten zu schützen und nicht rechtmäßige und gängige, sich aus der Netzwerkgestaltung ergebende Tätigkeiten oder rechtmäßige und gängige Betreiber- und Unternehmenspraktiken zu kriminalisieren.

Rechtswidriger Zugang (Artikel 2)

44. „Rechtswidriger Zugang“ umfasst gefährliche Bedrohungen und Angriffe gegen die Sicherheit (d. h. die Vertraulichkeit, Integrität und Verfügbarkeit) von Computersystemen und -daten als grundlegende Straftat. Das Schutzbedürfnis entsteht aus dem Interesse von Organisationen und Einzelpersonen, ihre Systeme ungestört und ungehindert verwalten, betreiben und kontrollieren zu können. Bloßes unbefugtes Eindringen, d. h. „Hacken“, „Knacken“ oder „Einschleichen“, soll grundsätzlich an sich rechtswidrig sein. Es kann zu Behinderungen für die rechtmäßigen Benutzer der Systeme und Daten führen und Veränderungen oder Zerstörung verbunden mit hohen Kosten für die Wiederherstellung verursachen. Ein solches Eindringen kann Zugang zu vertraulichen Daten (einschließlich Passwörtern, Informationen über das Zielsystem) und Geheimnissen und zur unentgeltlichen Nutzung des Systems verschaffen oder sogar Hacker dazu verleiten, gefährlichere Arten von Computerkriminalität wie Betrug oder Fälschung zu begehen.

45. Die wirkungsvollste Methode der Verhinderung unbefugten Zugriffs ist natürlich die Einführung und Entwicklung wirksamer Sicherheitsvorkehrungen. Ein umfassender Ansatz muss jedoch auch die Androhung und Anwendung strafrechtlicher Maßnahmen einschließen. Ein strafrechtliches Verbot des unbefugten Zugangs bietet für das System und die Daten als solche in einem frühen Stadium einen zusätzlichen Schutz vor den beschriebenen Gefahren.

46. „Zugang“ bedeutet die Öffnung zu einem Computersystem insgesamt oder zu einem Teil davon (Hardware, Komponenten, gespeicherte Daten des installierten Systems, Verzeichnisse, Verbindungs- und Inhaltsdaten). Nicht eingeschlossen ist jedoch das bloße Versenden einer E-Mail oder einer Datei an dieses System. „Zugang“ umfasst den Zugang zu einem anderen Computersystem über ein öffentliches Fernmeldenetz oder zu einem Computersystem im selben Netz wie in einem LAN („local area network“) oder in einem Intranet innerhalb einer Organisation. Die Art der Kommunikation (z. B. aus der Ferne, auch über drahtlose Verbindungen, oder aus der Nähe) spielt keine Rolle.

47. Die Handlung muss auch „unbefugt“ begangen werden. Neben der oben erläuterten Bedeutung dieses Begriffs besagt er auch, dass der vom Eigentümer oder rechtmäßigen Inhaber des Systems oder Systemteils genehmigte Zugang (z. B. zum Zweck des genehmigten Testens oder zum Schutz des betreffenden Computersystems) nicht kriminalisiert wird. Außerdem wird der Zugriff auf ein Computersystem, das den freien und offenen Zugriff durch die Öffentlichkeit erlaubt, nicht kriminalisiert, da ein solcher Zugang nicht unbefugt ist.

48. Die Verwendung bestimmter technischer Hilfsmittel kann zu einem Zugang nach Artikel 2 führen, so dem Zugriff auf eine Web-Seite, direkt oder über „hypertext links“ einschließlich „deep-links“ oder durch die Anwendung von „cookies“ oder „bots“ zur Abfrage von Informationen. Die Verwendung solcher Hilfsmittel ist nicht an sich „unbefugt“. Die Unterhaltung einer öffentlichen Website impliziert die Zustimmung des Website-Inhabers, dass diese für andere Benutzer des Web zugänglich ist. Die Verwendung von Standardhilfsmitteln, die in den gebräuchlichen Kommunikationsprotokollen und -programmen vorgesehen sind, ist als solche nicht „unbefugt“, insbesondere wenn davon auszugehen ist, dass der rechtmäßige Inhaber des besuchten Systems die Verwendung akzeptiert, indem er z. B. im Fall von „cookies“ die erste Installation nicht zurückweist oder löscht.

49. Viele innerstaatliche Gesetze enthalten bereits Vorschriften über „Hacking“-Straftaten, jedoch sind Geltungsbereich und Tatbestandsmerkmale sehr unter-

schiedlich. Der breit gefasste Ansatz im ersten Satz von Artikel 2 ist nicht unumstritten. Die Einwände betreffen Situationen, in denen das bloße Eindringen keine Gefahren verursacht hat oder wo sogar „Hacking“-Aktivitäten zur Aufdeckung von Lücken und Schwächen in der Sicherheit von Systemen geführt haben. Dies hat einige Länder dazu veranlasst, einen engeren Ansatz mit näher bezeichneten Voraussetzungen zu wählen, was auch der Empfehlung Nr. R (89) 9 und dem Vorschlag der OECD-Arbeitsgruppe von 1985 entspricht.

50. Die Vertragsparteien können den weit gefassten Ansatz wählen und nach Artikel 2 Satz 1 das bloße „Hacking“ kriminalisieren. Die Vertragsparteien können aber auch alle oder einzelne der in Satz 2 genannten ergänzenden Elemente voraussetzen: Verletzung von Sicherheitsmaßnahmen, die besondere Absicht, Computerdaten zu erlangen, andere unredliche Absicht, die die strafrechtliche Verantwortlichkeit begründet, oder die Voraussetzung, dass die Straftat in Zusammenhang mit einem Computersystem begangen worden sein muss, das mit einem anderen Computersystem verbunden ist. Letzteres ermöglicht es den Vertragsparteien, den Fall auszuschließen, in dem jemand auf einen einzelnen Computer ohne Benutzung eines anderen Computersystems physisch zugreift. Sie können die Straftat auf den rechtswidrigen Zugang auf vernetzte Computersysteme beschränken (einschließlich öffentlicher, von Telekommunikationsdiensten bereitgestellter Netze und privater Netze wie Intranets und Extranets).

Rechtswidriges Abfangen (Artikel 3)

51. Diese Vorschrift dient dem Schutz des Rechts auf Nichtöffentlichkeit der Datenübermittlung. Die Straftat erfasst dieselbe Verletzung der Nichtöffentlichkeit bei der Datenübermittlung wie beim traditionellen Abhören und Aufzeichnen von Telefongesprächen. Das Recht auf Achtung der Korrespondenz ist in Artikel 8 der Europäischen Menschenrechtskonvention verankert. Mit der nach Artikel 3 festgelegten Straftat wird dieser Grundsatz auf alle Formen der elektronischen Datenübertragung angewendet, sei es auf die Übertragung per Telefon, Fax, E-Mail oder Datei.

52. Der Wortlauf der Vorschrift wurde im Wesentlichen von dem Tatbestand des „unbefugten Abfangens“ in der Empfehlung Nr. R (89) 9 übernommen. Im vorliegenden Übereinkommen wird klargestellt, dass es bei den Kommunikationen um die „Übertragung von Computerdaten“ sowie die elektromagnetische Abstrahlung unter den nachstehend beschriebenen Umständen geht.

53. Das „mit technischen Hilfsmitteln bewirkte“ Abfangen bezieht sich auf das Abhören, Kontrollieren oder Überwachen des Inhalts von Kommunikationen, das Beschaffen des Inhalts von Daten unmittelbar durch Zugriff auf ein Computersystem und dessen Benutzung oder mittelbar durch Benutzung elektronischer Abhör- oder Abfanggeräte. Zum Abfangen kann auch das Aufzeichnen gehören. Technische Hilfsmittel schließen an Übertragungsleitungen angeschlossene technische Geräte ein sowie Geräte zur Erfassung und Aufzeichnung drahtloser Kommunikationen. Dazu gehören kann die Verwendung von Software, Passwörtern und Codes. Die Voraussetzung der Verwendung technischer Hilfsmittel ist eine Einschränkung, um die Überkriminalisierung zu vermeiden.

54. Die Straftat betrifft die „nichtöffentliche“ Übertragung von Computerdaten. Der Begriff „nichtöffentlich“ bezeichnet die Art des Übertragungs- (Kommunikations-) Vorgangs und nicht die Art der übertragenen Daten. Die übertragenen Daten mögen öffentlich zugängliche Informationen sein, jedoch möchten die Parteien vertraulich miteinander kommunizieren. Oder die Daten sollen aus kommerziellen Gründen geheim bleiben, bis für die Dienstleistung bezahlt wird, wie beim Pay-TV. Somit schließt der Begriff „nichtöffentlich“ als solcher nicht die Kommunikation über öffentliche Netze aus. Kommunikationen zwischen Betriebsangehörigen – sei es zu geschäftlichen Zwecken oder nicht –, die „nichtöffentliche Computerdatenübertragungen“ darstellen, sind ebenfalls nach Artikel 3 gegen unbefugtes Abfangen geschützt (siehe z. B. Urteil des EMRG in der Sache Halford ./. VK, 25. Juni 1997, 20605/92).

55. Die Kommunikation in Form der Übertragung von Computerdaten kann innerhalb desselben Computersystems (von der zentralen Recheneinheit auf den Bildschirm oder den Drucker) stattfinden, zwischen zwei derselben Person gehörenden Computersystemen, zwischen zwei miteinander kommunizierenden Computern oder zwischen einem Computer und einer Person (z. B. über die Tastatur). Dennoch können die Vertragsparteien als weiteres Element voraussetzen, dass die Kommunikation zwischen verbundenen Computersystemen übertragen wird.

56. Es wird darauf hingewiesen, dass die Tatsache, dass der Begriff „Computersystem“ auch Funkverbindungen einschließen kann, nicht bedeutet, dass eine Vertragspartei verpflichtet ist, das Abfangen einer Funkübertragung zu kriminalisieren, die zwar „nichtöffentlich“ ist, aber in einer relativ offenen und leicht zugänglichen Weise erfolgt und daher z. B. von Funkamateuren abgefangen werden kann.

57. Die Schaffung eines Straftatbestands in Bezug auf „elektromagnetische Abstrahlungen“ sorgt für einen umfassenderen Geltungsbereich. Elektromagnetische Abstrahlungen können von einem Computer während seines Betriebs ausgehen. Solche Abstrahlungen gelten nicht als „Daten“ im Sinne der Definition in Artikel 1. Jedoch können aus den Abstrahlungen Daten wiederhergestellt werden. Daher ist das Abfangen von Daten aus elektromagnetischen Abstrahlungen eines Computersystems in dieser Vorschrift als Straftat einbezogen.

58. Die Strafrechtliche Verantwortlichkeit ist gegeben, wenn das rechtswidrige Abfangen „vorsätzlich“ und „unbefugt“ begangen wird. Die Handlung ist gerechtfertigt, wenn die abfangende Person dazu berechtigt ist, wenn sie auf Anweisung oder mit Genehmigung der Teilnehmer der Übertragung handelt (einschließlich genehmigter Tests oder Schutzmaßnahmen, denen die Teilnehmer zugestimmt haben) oder wenn die Überwachung im Interesse der nationalen Sicherheit oder zur Aufdeckung von Straftaten durch die Ermittlungsbehörden gerechtfertigt ist. Auch wurde davon ausgegangen, dass die Anwendung gängiger handelsüblicher Praktiken wie die Verwendung von „cookies“ als solche nicht kriminalisiert werden soll, da es sich hier nicht um ein „unbefugtes“ Abfangen handelt. In Bezug auf nach Artikel 3 geschützte nichtöffentliche Kommunikationen von Betriebsangehörigen (siehe Nr. 54 oben) kann das innerstaatliche Recht Gründe für rechtmäßiges Abfangen solcher Kom-

munikationen vorsehen. Im Sinne von Artikel 3 würde das Abfangen unter derartigen Umständen als „nicht unbefugt“ angesehen werden.

59. In einigen Ländern kann das Abfangen eng verbunden sein mit dem rechtswidrigen Zugriff auf ein Computersystem. Um eine Übereinstimmung des Verbots und der Rechtsanwendung zu erreichen, können Länder, die nach Artikel 2 unredliche Absicht oder die Tatsache voraussetzen, dass die Straftat in Zusammenhang mit einem Computersystem begangen wird, das mit einem anderen Computersystem verbunden ist, ähnliche Merkmale als Voraussetzungen für die strafrechtliche Verantwortlichkeit auch nach diesem Artikel festlegen. Diese Merkmale sollen in Verbindung mit den anderen Merkmalen der Straftat wie „vorsätzlich“ und „unbefugt“ ausgelegt und angewandt werden.

Eingriff in Daten (Artikel 4)

60. Ziel dieser Vorschrift ist es, Computerdaten und Computerprogramme mit einem ähnlichen Schutz zu versehen wie ihn bewegliche Sachen vor vorsätzlicher Beschädigung genießen. Das geschützte Rechtsgut ist hier die Integrität und die sachgemäße Funktionsweise und Anwendung gespeicherter Computerdaten oder Computerprogramme.

61. In Absatz 1 beziehen sich „Beschädigen“ und „Beeinträchtigen“ als sich überschneidende Handlungen insbesondere auf eine negative Veränderung der Integrität oder des Informationsinhalts von Daten und Programmen. Die „Löschung“ von Daten entspricht der Zerstörung einer beweglichen Sache. Sie zerstört sie und macht sie unkenntlich. Das Unterdrücken von Computerdaten bedeutet jede Handlung, die die Verfügbarkeit der Daten für die Person mit Zugang zu dem Computer oder zu dem Datenträger, auf dem diese Daten gespeichert sind, verhindert oder beendet. Der Begriff „Veränderung“ bedeutet die Änderung vorhandener Daten. Die Eingabe von bösartigen Codes wie Viren und Trojanische Pferde ist daher in diesem Paragrafen erfasst ebenso wie die dadurch verursachte Änderung von Daten.

62. Die obigen Handlungen sind nur strafbar, wenn sie „unbefugt“ begangen werden. Gängige Tätigkeiten, die in der Netzwerkgestaltung begründet sind, oder gängige Betriebs- oder Unternehmenspraktiken wie z. B. zur Prüfung der Sicherheit oder zum Schutz eines Computersystems mit Genehmigung des Eigentümers oder Betreibers oder zur Neukonfiguration eines Betriebssystems, wenn der Betreiber eines Systems eine neue Software erwirbt (z. B. Software, die den Zugang zum Internet gestattet und die ähnliche, zuvor installierte Programme unbrauchbar macht), sind keine unbefugten Handlungen und werden daher durch diesen Artikel nicht kriminalisiert. Die Änderung von Verbindungsdaten zur Erleichterung anonymer Kommunikationen (z. B. die Aktivitäten anonymer Remailer-Systeme) oder die Änderung von Daten zum Zweck der sicheren Kommunikation (z. B. Verschlüsselung) sollten grundsätzlich als legitimer Datenschutz und damit als berechtigt vorgenommen angesehen werden. Die Vertragsparteien möchten jedoch möglicherweise bestimmte Formen des Missbrauchs in Zusammenhang mit anonymen Kommunikationen kriminalisieren, so z. B. die Veränderung der Kopfdaten eines Pakets, um die Identität des Täters bei Begehung einer Straftat zu verbergen.

63. Außerdem muss der Täter „vorsätzlich“ gehandelt haben.

64. Absatz 2 erlaubt es den Vertragsparteien, zu dieser Straftat einen Vorbehalt einzulegen, indem sie als Voraussetzung vorsehen, dass das Verhalten zu einem schweren Schaden geführt haben muss. Was unter einem schweren Schaden zu verstehen ist, bleibt der innerstaatlichen Gesetzgebung überlassen, jedoch sollen die Vertragsparteien dem Generalsekretär des Europarats die Auslegung notifizieren, falls sie von der Möglichkeit des Vorbehalts Gebrauch machen.

Eingriff in ein System (Artikel 5)

65. Dies wird in der Empfehlung Nr. R (89) 9 als Computersabotage bezeichnet. Die Vorschrift bezweckt die Kriminalisierung der vorsätzlichen Behinderung der rechtmäßigen Benutzung von Computersystemen einschließlich Telekommunikationsanlagen durch Verwendung oder Beeinflussung von Computerdaten. Das geschützte Rechtsgut ist das Interesse der Betreiber und Benutzer von Computer- oder Telekommunikationssystemen an deren ordnungsgemäßer Funktionsweise. Die Vorschrift ist neutral formuliert, damit alle Arten von Funktionen geschützt werden können.

66. Der Begriff „Behinderung“ bezeichnet Handlungen, welche die ordnungsgemäße Funktionsweise des Computersystems stören. Eine derartige Behinderung soll durch Eingeben, Übermitteln, Beschädigen, Löschen, Verändern oder Unterdrücken von Computerdaten erfolgen.

67. Die Behinderung muss außerdem „schwer“ sein, um strafrechtliche Sanktionen auszulösen. Jede Vertragspartei legt für sich selbst fest, welche Kriterien erfüllt sein müssen, damit die Behinderung als „schwer“ angesehen werden kann. Eine Vertragspartei kann z. B. festlegen, dass ein Mindestmaß an Beschädigung verursacht worden sein muss, damit die Behinderung als schwer angesehen werden kann. Die Verfasser sahen es als schwere Behinderung an, wenn Daten in einer Form, einem Umfang oder einer Häufigkeit an ein bestimmtes System versandt werden, die eine erhebliche schädliche Auswirkung auf die Fähigkeit des Eigentümers oder Betreibers haben, das System zu benutzen oder mit anderen Systemen zu kommunizieren (z. B. mit Programmen, die Angriffe in Form der „Dienstverweigerung“ erzeugen, bösartige Codes wie Viren, die den Betrieb des Systems verhindern oder wesentlich verlangsamen, oder Programme, die riesige Mengen elektronischer Post an einen Empfänger senden, um die Kommunikationsfunktionen des Systems zu blockieren).

68. Die Behinderung muss „unbefugt“ erfolgen. In der Netzwerkgestaltung begründete gängige Aktivitäten oder gängige Betreiber- oder Unternehmenspraktiken sind nicht unbefugt. Dazu gehört z. B. die Prüfung der Sicherheit oder der Schutz eines Computersystems mit Genehmigung des Eigentümers oder Betreibers oder die Neukonfiguration des Betriebssystems, wenn der Betreiber des Systems eine neue Software installiert, die ähnliche, zuvor installierte Programme unbrauchbar macht. Daher werden derartige Handlungen durch diesen Artikel nicht kriminalisiert, selbst wenn sie eine schwere Behinderung verursachen.

69. Das Versenden unangeforderter E-Mails zu kommerziellen oder anderen Zwecken kann für die Empfänger

eine Belästigung sein, insbesondere wenn solche Nachrichten in großen Mengen oder mit hoher Frequenz versandt werden („spamming“). Nach Meinung der Verfasser soll ein solches Verhalten nur dann kriminalisiert werden, wenn die Kommunikation vorsätzlich und schwer behindert wird. Jedoch können die Vertragsparteien in ihrem innerstaatlichen Recht die Frage der Behinderung unterschiedlich regeln, indem sie z. B. bestimmte Eingriffshandlungen zu Ordnungswidrigkeiten machen oder auf andere Weise mit Sanktionen belegen. Der Wortlaut überlässt es den Vertragsparteien festzulegen, in welchem Umfang der Betrieb des Systems behindert sein muss – teilweise oder vollständig, vorübergehend oder auf Dauer –, um die Schadensgrenze zu erreichen, die eine verwaltungsrechtliche oder strafrechtliche Sanktion nach ihren Rechtsvorschriften rechtfertigt.

70. Die Straftat muss vorsätzlich begangen werden, d. h. der Täter muss den Vorsatz haben, eine schwere Behinderung zu verursachen.

Missbrauch von Vorrichtungen (Artikel 6)

71. Diese Bestimmung macht die vorsätzliche Begehung bestimmter rechtswidriger Handlungen bezüglich bestimmter Vorrichtungen oder Zugriffsdaten, die zur Begehung der oben genannten Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen missbraucht werden sollen, zu einem gesonderten, eigenständigen Straftatbestand. Da die Begehung dieser Straftaten häufig den Besitz von Zugriffsmitteln („Hackerwerkzeugen“) oder anderen Werkzeugen voraussetzt, ist ein starker Anreiz gegeben, sich diese zu kriminellen Zwecken zu beschaffen, was dann zu einer Art Schwarzmarkt bei der Herstellung und Verbreitung führen kann. Um dieser Gefahr wirksamer begegnen zu können, sollte das Strafrecht bestimmte potenziell gefährliche, der Begehung der Straftaten nach Artikel 2 bis 5 vorausgehende Handlungen an der Quelle verbieten. Diese Bestimmung folgt hier jüngsten Entwicklungen im Europarat (Europäisches Übereinkommen über Rechtsschutz für Dienstleistungen mit bedingtem Zugang und der Dienstleistungen zu bedingtem Zugang – ETS Nr. 178) und in der Europäischen Union (Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. November 1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten) sowie einschlägigen Bestimmungen in einigen Ländern. Ein ähnlicher Ansatz findet sich bereits im Genfer Abkommen von 1929 über Falschmünzerei.

72. Absatz 1 Buchstabe a Ziffer 1 kriminalisiert das Herstellen, Verkaufen, Beschaffen zwecks Gebrauch, Einführen, Verbreiten oder anderweitige Verfügbarmachen einer Vorrichtung einschließlich eines Computerprogramms, die in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine der nach den Artikeln 2 bis 5 des Übereinkommens umschriebenen Straftaten zu begehen. „Verbreiten“ bezieht sich auf die aktive Handlung der Weitergabe von Daten an andere, während „Zugänglichmachen“ das Online-Stellen von Vorrichtungen zum Gebrauch durch andere meint. Dieser Begriff soll auch die Schaffung oder Zusammenstellung von Hyperlinks abdecken, die den Zugriff auf derartige Vorrichtungen erleichtern. Die Einbeziehung eines „Computerprogramms“ bezieht sich auf Programme, die z. B. dazu bestimmt sind, Daten zu verändern oder sogar zu löschen oder den Betrieb eines Systems zu stören, wie z. B. Virusprogramme, oder Programme, die dafür konstruiert oder bearbeitet wurden, den Zugriff auf Computersysteme zu ermöglichen.

73. Die Verfasser diskutierten ausführlich, ob die Vorrichtungen auf solche beschränkt werden sollten, die ausschließlich oder speziell für die Begehung von Straftaten bestimmt sind, und somit Mehrzweckvorrichtungen ausgeschlossen wären. Dies wurde als zu eng angesehen. Es könnte zu unüberwindlichen Beweisschwierigkeiten im Strafverfahren führen und die Bestimmung praktisch unanwendbar oder nur in seltenen Fällen anwendbar machen. Die Alternative, alle Vorrichtungen einzubeziehen, auch wenn sie rechtmäßig hergestellt und verbreitet werden, wurde ebenfalls abgelehnt. Nur das subjektive Element des Vorsatzes, eine Computerstraftat zu begehen, wäre dann für die Verhängung einer Strafe entscheidend, ein Ansatz, der auch im Bereich der Geldfälschung nicht verfolgt wurde. Ein vernünftiger Kompromiss besteht darin, den Geltungsbereich des Übereinkommens auf Fälle zu beschränken, in denen die Vorrichtungen objektiv in erster Linie zu dem Zweck konstruiert oder bearbeitet worden sind, um eine Straftat zu begehen. Dies allein schon wird gewöhnlich Mehrzweckvorrichtungen ausschließen.

74. Absatz 1 Buchstabe a Ziffer 2 kriminalisiert das Herstellen, Verkaufen, Beschaffen zwecks Gebrauch, Einführen, Verbreiten oder anderweitige Verfügbarmachen eines Computerpassworts, eines Zugangscodes oder ähnlicher Daten, die den Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon ermöglichen.

75. Absatz 1 Buchstabe b begründet den Besitz eines Mittels nach Absatz 1 Buchstabe a Ziffer 1 oder 2 als Straftat. Gemäß dem letzten Satz von Buchstabe b können die Vertragsparteien in ihrem Recht voraussetzen, dass eine bestimmte Anzahl dieser Mittel in jemandes Besitz sein muss. Die Anzahl dieser Mittel ist zugleich der Nachweis für den strafrechtlichen Vorsatz. Jede Vertragspartei kann die Anzahl bestimmen, welche die strafrechtliche Verantwortlichkeit begründet.

76. Der Straftatbestand setzt voraus, dass die Tat vorsätzlich und unbefugt begangen worden sein muss. Um die Gefahr der Überkriminalisierung zu vermeiden, wenn Vorrichtungen zu rechtmäßigen Zwecken hergestellt und auf den Markt gebracht werden, z. B. zu Gegenangriffen gegen Computersysteme, werden weitere Elemente hinzugefügt, um den Straftatbestand einzuschränken. Neben dem allgemeinen Vorsatz muss auch ein besonderer (d.h. direkter Vorsatz) gegeben sein, die Vorrichtung zur Begehung einer der in den Artikeln 2 bis 5 genannten Straftaten zu verwenden.

77. Absatz 2 macht deutlich, dass Werkzeuge, die für das befugte Testen oder für den Schutz des Computersystems geschaffen wurden, nicht von dieser Bestimmung erfasst werden. Dies ist schon in dem Ausdruck „unbefugt“ enthalten. So werden z. B. Testvorrichtungen („Knackvorrichtungen“) und Vorrichtungen für die Netzanalyse, die von der Industrie verwendet werden, um die Zuverlässigkeit ihrer Informationstechnologieprodukte zu kontrollieren oder um die Systemsicherheit zu prüfen, zu rechtmäßigen Zwecken hergestellt und als „befugt“ verwendet angesehen.

78. Wegen der unterschiedlichen Beurteilung der Notwendigkeit, den Straftatbestand Missbrauch von Vorrichtungen auf alle Arten von Computerstraftaten nach Arti-

kel 2 bis 5 anzuwenden, gestattet es Absatz 3, auf der Grundlage eines Vorbehalts (vgl. Artikel 42) den Straftatbestand im innerstaatlichen Recht einzuschränken. Jede Vertragspartei ist jedoch verpflichtet, zumindest das Verkaufen, Verbreiten oder Zugänglichmachen eines Computerpassworts oder von Zugangsdaten nach Absatz 1 Buchstabe a Ziffer 2 zu kriminalisieren.

Titel 2
Computerbezogene Straftaten

79. Die Artikel 7 bis 10 beziehen sich auf allgemeine Straftaten, die häufig unter Verwendung eines Computersystems begangen werden. Die meisten Staaten haben bereits diese allgemeinen Straftaten kriminalisiert und ihre bestehenden Rechtsvorschriften mögen hinreichend weit gefasst sein, um auch die Fälle abdecken zu können, in denen Computernetzwerke verwendet werden – oder auch nicht (z. B. können die Rechtsvorschriften einiger Staaten über Kinderpornografie nicht auf elektronische Bilder angewandt werden). Daher müssen die Staaten bei der Umsetzung dieser Artikel ihre bestehenden Rechtsvorschriften daraufhin prüfen, ob sie auf Fälle Anwendung finden, in denen Computersysteme oder -netze verwendet werden. Wenn die bestehenden Straftatbestände bereits derartige Handlungen abdecken, ist es nicht erforderlich, die bestehenden Straftatbestände zu ändern oder neue zu schaffen.

80. „Computerbezogene Fälschung“ und „Computerbezogener Betrug“ behandeln bestimmte Computerstraftaten, nämlich Computerurkundenfälschung und Computerbetrug als zwei spezielle Formen der Manipulation von Computersystemen oder Computerdaten. Mit ihrer Aufnahme wird dem Umstand Rechnung getragen, dass bestimmte traditionelle Rechtsgüter in vielen Ländern vor neuartigen Störungen und Angriffen nicht hinreichend geschützt sind.

Computerbezogene Fälschung (Artikel 7)

81. Der Zweck dieses Artikels ist, einen parallelen Straftatbestand zur Fälschung verkörperter Urkunden zu schaffen. Mit ihm sollen strafrechtliche Lücken bei der herkömmlichen Urkundenfälschung beseitigt werden; sie setzt die visuelle Lesbarkeit der in einer Urkunde enthaltenen Angaben oder Erklärungen voraus und trifft auf elektronisch gespeicherte Daten nicht zu. Veränderungen solcher beweiserheblicher Daten können dieselben ernsten Folgen haben wie herkömmliche Fälschungshandlungen, wenn ein Dritter durch sie irregeführt wird. Computerbezogenene Fälschung umfasst das unbefugte Herstellen oder Verändern gespeicherter Daten, so dass sie einen anderen Beweiswert annehmen und der Verlauf der Rechtsgeschäfte, bei dem auf die Echtheit der in den Daten enthaltenen Angaben vertraut wird, von einer Täuschung abhängt. Geschütztes Rechtsgut ist die Sicherheit und Zuverlässigkeit elektronischer Daten, die für den Rechtsverkehr Folgen haben können.

82. Es ist zu beachten, dass die nationalen Begriffe der Urkundenfälschung erheblich voneinander abweichen. Ein Begriff geht von der Authentizität in Bezug auf den Verfasser der Urkunde aus, andere von der Wahrheit der in der Urkunde enthaltenen Angaben. Man war sich jedoch einig, dass die Täuschung in Bezug auf die Echtheit sich mindestens auf denjenigen bezieht, der die Daten ausgibt, ungeachtet der Richtigkeit oder Wahrheit des Inhalts der Daten. Die Vertragsparteien können darüber hinausgehen und in den Begriff „echt“ auch die Unverfälschtheit der Daten einbeziehen.

83. Diese Bestimmung erstreckt sich auf Daten, die einer mit Rechtsfolgen verbundenen öffentlichen oder privaten Urkunde gleichstehen. Die unbefugte „Eingabe“ richtiger oder unrichtiger Daten führt zu einer Situation, die dem Herstellen einer falschen Urkunde entspricht. Späteres Verändern (Abwandeln, Variieren, teilweises Umändern), Löschen (Entfernen der Daten von einem Datenträger) und Unterdrücken (Zurückhalten, Verbergen von Daten) entspricht im Allgemeinen dem Verfälschen einer echten Urkunde.

84. Der Ausdruck „für rechtliche Zwecke“ bezieht sich auch auf Rechtsgeschäfte und rechtserhebliche Schriftstücke.

85. Der letzte Satz der Bestimmung ermöglicht es den Vertragsparteien, bei der Umsetzung des Straftatbestands in ihr innerstaatliches Recht als weitere Voraussetzung für die Strafbarkeit eine betrügerische oder ähnliche unredliche Absicht vorzusehen.

Computerbezogener Betrug (Artikel 8)

86. Mit dem Beginn der technischen Revolution haben sich die Gelegenheiten zur Begehung von Wirtschaftsstraftaten wie Betrug einschließlich Kreditkartenbetrug vervielfacht. In Computersystemen dargestelltes oder verwaltetes Vermögen (elektronische Zahlungsmittel, Buchgeld) ist zum Ziel von Manipulationen geworden, wie dies auch bei herkömmlichen Vermögensformen der Fall ist. Bei diesen Straftaten handelt es sich hauptsächlich um Eingabemanipulationen, indem unrichtige Daten in den Computer eingegeben werden, oder um Programmmanipulationen oder sonstige Eingriffe in den Ablauf der Datenverarbeitung. Ziel dieses Artikels ist, jede unzulässige Manipulation im Datenverarbeitungsvorgang, die in der Absicht vorgenommen wird, eine rechtswidrige Vermögensübertragung zu bewirken, mit Strafe zu bedrohen.

87. Damit sichergestellt ist, dass alle möglichen einschlägigen Manipulationen erfasst sind, werden die Tatbestandsmerkmale „Eingeben“, „Verändern“, „Löschen“ oder „Unterdrücken“ in Artikel 8 Buchstabe a ergänzt durch die allgemeine Handlung des „Eingreifens in den Betrieb eines Computersystems“ in Artikel 8 Buchstabe b. Die Merkmale „Eingeben, Verändern, Löschen oder Unterdrücken“ haben dieselbe Bedeutung wie in den vorstehenden Artikeln. Artikel 8 Buchstabe b umfasst Handlungen wie Manipulationen der Hardware, Handlungen, mit denen Ausdrucke unterdrückt werden, und Handlungen, welche die Datenaufzeichnung oder den Datenfluss oder die Reihenfolge, in welcher die Programme ablaufen, beeinflussen.

88. Computerbetrugshandlungen sind mit Strafe bedroht, wenn sie zu einer unmittelbaren wirtschaftlichen oder besitzrechtlichen Beschädigung des Vermögens eines anderen führen und der Täter in der Absicht gehandelt hat, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen. Der Ausdruck „Vermögensschaden“ ist ein weitgefasster Begriff und schließt den Verlust von Geld sowie materiellen und immateriellen Positionen mit wirtschaftlichem Wert ein.

89. Die Straftat muss „unbefugt“ begangen und der Vermögensvorteil unbefugt erlangt worden sein. Selbstverständlich sollen zulässige, im Handelsverkehr übliche

Praktiken, die darauf gerichtet sind, einen Vermögensvorteil zu erlangen, nicht unter die nach diesem Artikel festgelegte Straftat fallen, da sie nicht unbefugt durchgeführt werden. So sind beispielsweise Aktivitäten, die nach einem gültigen Vertrag zwischen den betroffenen Personen durchgeführt werden, nicht unbefugt (z. B. die Sperrung einer Website aufgrund einer vertraglich bestimmten Befugnis).

90. Die Straftat muss „vorsätzlich" begangen worden sein. Das allgemeine Merkmal des Vorsatzes bezieht sich auf die Computermanipulation oder den Eingriff, die den Vermögensschaden bei einem anderen verursachen. Die Straftat setzt ferner eine bestimmte (betrügerische oder andere unredliche) Absicht voraus, sich oder einem Dritten einen Vermögensvorteil zu verschaffen. So sollen zum Beispiel Handelspraktiken in Bezug auf den Wettbewerb, die einen wirtschaftlichen Nachteil für den einen und einen Vorteil für den anderen mit sich bringen, aber nicht in betrügerischer oder unredlicher Absicht angewandt werden, nicht von der nach diesem Artikel festgelegten Straftat erfasst werden. Zum Bespiel soll die Verwendung von Informationsbeschaffungsprogrammen bei der vergleichenden Warenprüfung im Internet („bots"), auch wenn die Berechtigung dazu von der vom „bot" besuchten Website nicht vorliegt, nicht kriminalisiert werden.

Titel 3
Inhaltsbezogene Straftaten

Straftaten mit Bezug zu Kinderpornografie (Artikel 9)

91. Mit Artikel 9 über Kinderpornografie sollen Maßnahmen zum Schutz von Kindern, einschließlich ihres Schutzes vor sexueller Ausbeutung, dadurch gestärkt werden, dass strafrechtliche Bestimmungen modernisiert werden, um die Nutzung von Computersystemen bei der Begehung sexueller Straftaten gegen Kinder wirksamer einzugrenzen.

92. Diese Bestimmung nimmt Bezug auf die Besorgnis der Staats- und Regierungschefs des Europarats, wie sie in dem bei ihrem 2. Gipfeltreffen (Straßburg, 10. – 11. Oktober 1997) verabschiedeten Aktionsplan (Punkt III.4) zum Ausdruck gebracht wurde, und entspricht dem internationalen Trend hin zum Verbot der Kinderpornografie, der durch die kürzlich erfolgte Verabschiedung des Fakultativprotokolls zum Übereinkommen der Vereinten Nationen über die Rechte des Kindes, Kinderhandel, Kinderprostitution und Kinderpornografie sowie die jüngste Initiative der Europäischen Kommission zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie (COM2000/854) belegt wird.

93. In dieser Bestimmung werden verschiedene Aspekte der elektronischen Herstellung, des elektronischen Besitzes und der elektronischen Verbreitung von Kinderpornografie unter Strafe gestellt. Zwar haben die meisten Staaten die herkömmliche Herstellung und physische Verbreitung von Kinderpornografie bereits unter Strafe gestellt, aber da das Internet immer mehr zum wichtigsten Hilfsmittel für den Handel mit solchem Material wird, war man der Meinung, dass spezifische Rechtsvorschriften in einem internationalen Rechtsinstrument dringend erforderlich seien, um diese Form der sexuellen Ausbeutung und der Gefährdung von Kindern zu bekämpfen. In weiten Kreisen ist man der Überzeugung, dass dieses Material sowie der online erfolgende Austausch von Ideen, Fantasien und Ratschlägen zwischen Pädophilen dazu beiträgt, sexuelle Straftaten gegen Kinder zu unterstützen, zu fördern oder zu erleichtern.

94. In Absatz 1 Buchstabe a wird das Herstellen von Kinderpornografie zum Zweck ihrer Verbreitung über ein Computersystem als Straftat festgelegt. Diese Bestimmung hielt man für erforderlich, um die oben beschriebenen Gefahren an der Quelle zu bekämpfen.

95. In Absatz 1 Buchstabe b wird das „Anbieten" von Kinderpornografie über ein Computersystem als Straftat festgelegt. Der Begriff „Anbieten" soll auch die Werbung an andere, sich Kinderpornografie zu beschaffen, abdecken. Der Begriff impliziert, dass die Person, die das Material anbietet, dieses tatsächlich liefern kann. Der Begriff „Verfügbarmachen" soll auch das Online-Stellen von Kinderpornografie zum Zweck ihrer Verwendung durch andere, beispielsweise durch die Einrichtung von Kinderpornografie-Internetseiten, abdecken. Dieser Absatz soll auch die Schaffung oder Zusammenstellung von Hyperlinks zu kinderpornografischen Seiten zur Erleichterung des Zugangs zur Kinderpornografie erfassen.

96. In Absatz 1 Buchstabe c wird das Verbreiten oder Übermitteln von Kinderpornografie über ein Computersystem als Straftat erfasst. Mit „Verbreiten" ist die aktive Weiterverbreitung des Materials gemeint. Das Versenden von Kinderpornografie an eine andere Person mittels eines Computersystems würde als eine Straftat des „Übermittelns" von Kinderpornografie behandelt.

97. Der Ausdruck „Beschaffen für sich selbst oder einen anderen" in Absatz 1 Buchstabe d erfasst die aktive Beschaffung von Kinderpornografie, beispielsweise durch das Herunterladen.

98. Der Besitz von Kinderpornografie in einem Computersystem oder auf einem Datenträger wie beispielsweise einer Diskette oder CD-ROM wird in Absatz 1 Buchstabe e als Straftat festgelegt. Der Besitz von Kinderpornografie regt die Nachfrage nach derartigem Material an. Eine wirksame Methode zur Eindämmung der Herstellung von Kinderpornografie besteht darin, an das Verhalten jeder Person, die in der Kette von der Herstellung bis zum Besitz eine Rolle spielt, strafrechtliche Folgen zu knüpfen.

99. Der in Absatz 2 verwendete Begriff „pornografisches Material" wird durch die innerstaatlichen Normen zur Klassifizierung von Materialien als obszön, mit der öffentlichen Moral unvereinbar oder in ähnlicher Weise verdorben definiert. Daher ist Material, das einen künstlerischen, medizinischen, wissenschaftlichen oder ähnlichen Wert hat, möglicherweise nicht als pornografisch einzustufen. Zur visuellen Darstellung zählen auch Daten, die auf einer Computerdiskette oder in einem anderen elektronischen Speichermedium gespeichert sind und in ein visuelles Bild konvertiert werden können.

100. Die „sexuell eindeutige Handlung" erfasst wenigstens, ob tatsächlich oder vorgetäuscht, a) den Geschlechtsverkehr, einschließlich genital-genitalem Verkehr, oral-genitalem, anal-genitalem oder oral-analem Verkehr, zwischen Minderjährigen oder zwischen einem Minderjährigen und einem Erwachsenen gleichen oder des anderen Geschlechts, b) Sodomie, c) Masturbation, d) sadistischen oder masochistischen Missbrauch in einem sexuellen Kontext und e) laszive Entblößung der

Geschlechtsteile oder der Schamgegend von Minderjährigen. Es spielt keine Rolle, ob eine tatsächliche oder vorgetäuschte Handlung dargestellt ist.

101. Die drei Arten von Material, die in Absatz 2 zum Zwecke der Festlegung des Tatbestands bezüglich der in Absatz 1 aufgeführten Straftaten definiert sind, umfassen Darstellungen des sexuellen Missbrauchs eines wirklichen Kindes (Buchstabe a), pornografische Bilder, die eine Person darstellen, die als ein Kind bei sexuell eindeutigen Handlungen erscheint, (Buchstabe b) und schließlich Bilder, die zwar „realistisch" sind, bei denen aber nicht tatsächlich ein Kind bei sexuell eindeutigen Handlungen beteiligt ist (Buchstabe c). Zu dem letztgenannten Szenario gehören Bilder, an denen Änderungen vorgenommen wurden, wie z. B. morphisierte Bilder von natürlichen Personen, oder auch Bilder, die allein mit dem Computer erstellt wurden.

102. In den drei in Absatz 2 geschilderten Fällen werden leicht unterschiedliche rechtliche Interessen geschützt. In Absatz 2 Buchstabe a geht es unmittelbarer um den Schutz vor Kindesmissbrauch. Die Buchstaben b und c zielen auf den Schutz vor einem Verhalten, durch das nicht notwendigerweise dem in dem Material dargestellten „Kind" ein Schaden zugefügt wird, da es sich ja vielleicht nicht um ein wirkliches Kind handelt, das jedoch dazu führen kann, dass Kinder ermutigt oder verführt werden, an solchen Handlungen teilzunehmen, und das daher einen Teil der Subkultur darstellt, durch die der Kindesmissbrauch gefördert wird.

103. Der Begriff „unbefugt" schließt gesetzlich vorgesehene Ausnahmen und Schuldausschließungsgründe, Rechtfertigungsgründe oder ähnliche Grundsätze, nach denen eine Person unter bestimmten Voraussetzungen von der strafrechtlichen Verantwortlichkeit befreit ist, nicht aus. Daher ermöglicht der Begriff „unbefugt" einer Vertragspartei, Grundrechte wie die Gedankenfreiheit, die Freiheit der Meinungsäußerung und das Recht auf Wahrung der Privatsphäre zu berücksichtigen. Zusätzlich kann eine Vertragspartei noch eine Ausnahme in Bezug auf „pornografisches Material" vorsehen, das einen künstlerischen, medizinischen, wissenschaftlichen oder ähnlichen Wert hat. In Bezug auf Absatz 2 Buchstabe b dürfte der Begriff „unbefugt" einer Vertragspartei beispielsweise gestatten, eine Person von der strafrechtlichen Verantwortlichkeit zu befreien, wenn der Nachweis erbracht ist, dass es sich bei der dargestellten Person nicht um eine minderjährige Person im Sinne dieser Vorschrift handelt.

104. In Übereinstimmung mit der Definition eines „Kindes" in dem Übereinkommen der Vereinten Nationen über die Rechte des Kindes (Artikel 1) umfasst der Begriff „minderjährige Person" nach Absatz 3 im Hinblick auf die Kinderpornografie allgemein alle Personen unter 18 Jahren. Man war der Auffassung, dass es aus grundsätzlichen Erwägungen wichtig sei, hinsichtlich des Alters eine einheitliche internationale Norm zu schaffen. Dabei sollte bedacht werden, dass sich das Alter auf die Benutzung von (wirklichen oder fiktiven) Kindern als Sexualobjekte bezieht, und von dem Alter zu unterscheiden ist, in dem man in eine sexuelle Beziehung einwilligen kann. Dennoch ermöglicht, in Anerkennung der Tatsache, dass einige Staaten in ihren innerstaatlichen Rechtsvorschriften über die Kinderpornografie ein niedrigeres Alter voraussetzen, der letzte Satz von Absatz 3 den Vertragsparteien, eine andere Altersgrenze festzusetzen, die jedoch 16 Jahre nicht unterschreiten darf.

105. In diesem Artikel werden verschiedene Arten von unerlaubten Handlungen im Zusammenhang mit Kinderpornografie aufgelistet, welche die Vertragsparteien ebenso wie in den Artikeln 2 bis 8 als Straftat erfassen müssen, wenn sie „vorsätzlich" begangen werden. Nach diesem Kriterium ist eine Person strafrechtlich nicht verantwortlich, wenn sie nicht den Vorsatz hatte, Kinderpornografie anzubieten, zur Verfügung zu stellen, zu vertreiben, zu übermitteln, herzustellen oder zu besitzen. Die Vertragsparteien könnten konkretere Vorschriften erlassen (siehe beispielsweise die anwendbaren Rechtsvorschriften der Europäischen Union im Hinblick auf die Verantwortlichkeit von Diensteanbietern); diese hätten dann Vorrang. Man könnte beispielsweise vorsehen, dass eine strafrechtliche Verantwortlichkeit dann vorliegt, wenn eine „Kenntnis und tatsächliche Beherrschung" hinsichtlich der Informationen gegeben ist, die übermittelt oder gespeichert werden. Es genügt beispielsweise nicht, dass ein Diensteanbieter nur als Übermittler solchen Materials dient oder nur Anbieter einer Internetseite oder eines Newsroom ist, der solches Material enthält, wenn in dem konkreten Fall kein Vorsatz nach den innerstaatlichen Rechtsvorschriften bestand. Außerdem ist ein Diensteanbieter nach diesem Artikel nicht verpflichtet, Handlungen zu überwachen, um eine strafrechtliche Verantwortlichkeit zu vermeiden.

106. Nach Absatz 4 haben die Vertragsparteien in Bezug auf Absatz 1 Buchstaben d und e und Absatz 2 Buchstaben b und c ein Vorbehaltsrecht. Das Recht, diese Teile der Bestimmung nicht anzuwenden, kann ganz oder teilweise ausgeübt werden. Ein solcher Vorbehalt soll gemäß Artikel 42 bei der Unterzeichnung oder bei der Hinterlegung der Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde der Vertragspartei gegenüber dem Generalsekretär des Europarats erklärt werden.

Titel 4
Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte

Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte (Artikel 10)

107. Verletzungen von Rechten des geistigen Eigentums, insbesondere des Urheberrechts, gehören zu den am häufigsten begangenen Straftaten im Internet, die sowohl den Inhabern von Urheberrechten als auch denjenigen Sorge bereiten, die sich beruflich mit Computernetzen beschäftigen. Die vom Inhaber des Urheberrechts nicht genehmigte Vervielfältigung und Veröffentlichung geschützter Werke im Internet kommt äußerst häufig vor. Solche geschützten Werke schließen literarische, fotografische, musikalische, audiovisuelle und andere Werke ein. Die Leichtigkeit, mit der mittels digitaler Technik unbefugte Kopien angefertigt werden können, sowie das Ausmaß der Vervielfältigung und Veröffentlichung im Rahmen elektronischer Netzwerke haben es nötig gemacht, Bestimmungen über strafrechtliche Sanktionen aufzunehmen und die internationale Zusammenarbeit auf diesem Gebiet zu verstärken.

108. Jede Vertragspartei ist verpflichtet, vorsätzliche Verletzungen des Urheberrechts und verwandter Schutz-

rechte, die sich aus den in dem Artikel aufgeführten Übereinkünften ergeben, mit Strafe zu bedrohen, wenn solche Verletzungen mittels eines Computersystems und „in gewerbsmäßigem Umfang“ begangen werden. Absatz 1 sieht strafrechtliche Sanktionen bei Verletzungen des Urheberrechts mittels eines Computersystems vor. Urheberrechtsverletzungen stellen bereits in fast allen Staaten eine Straftat dar. Absatz 2 behandelt die Verletzung verwandter Schutzrechte mittels eines Computersystems.

109. Verletzungen sowohl des Urheberrechts als auch verwandter Schutzrechte richten sich begrifflich nach dem innerstaatlichen Recht der jeweiligen Vertragspartei und nach den Verpflichtungen, welche die Vertragspartei in Bezug auf bestimmte internationale Übereinkünfte übernommen hat. Zwar wird von jeder Vertragspartei verlangt, dass sie diese Verletzungen als Straftaten festlegt, doch wie diese Verletzungen im Einzelnen nach innerstaatlichem Recht definiert sind, kann von Staat zu Staat unterschiedlich sein. Verpflichtungen zur Kriminalisierung nach dem Übereinkommen erstrecken sich jedoch nur auf die in Artikel 10 ausdrücklich genannten Verletzungen des geistigen Eigentums und schließen somit Verletzungen in Bezug auf Patente oder Warenzeichen aus.

110. Die Übereinkünfte, auf die in Absatz 1 Bezug genommen wird, sind die Pariser Fassung vom 24. Juli 1971 der Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst, das Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums (TRIPS) und das Urheberrechtsübereinkommen der Weltorganisation für geistiges Eigentum (WIPO). Die in Absatz 2 genannten internationalen Übereinkünfte sind das Internationale Abkommen über den Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendeunternehmen (Abkommen von Rom), das Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums (TRIPS) und der WIPO-Vertrag betreffend Darbietungen und Tonträger. Durch die Verwendung der Worte „aufgrund ihrer Verpflichtungen“ in beiden Absätzen wird klargestellt, dass eine Vertragspartei dieses Übereinkommens nicht verpflichtet ist, aufgeführte Übereinkünfte anzuwenden, bei denen sie nicht Vertragspartei ist; ferner gilt, dass, soweit eine Vertragspartei einen nach einer dieser Übereinkünfte zulässigen Vorbehalt angebracht oder eine entsprechende Erklärung abgegeben hat, dieser Vorbehalt den Umfang ihrer Verpflichtung nach diesem Übereinkommen eingrenzen kann.

111. Das WIPO-Urheberrechtsübereinkommen und der WIPO-Vertrag betreffend Darbietungen und Tonträger waren noch nicht in Kraft, als dieses Übereinkommen geschlossen wurde. Gleichwohl sind diese Übereinkünfte wichtig, da sie den internationalen Schutz des geistigen Eigentums (insbesondere im Hinblick auf das neue Recht des „Zugänglichmachens“ von geschütztem Material „auf Anfrage“ über das Internet) deutlich aktualisieren und die Mittel zur Bekämpfung von Verstößen gegen Rechte des geistigen Eigentums weltweit verbessern. Es wird jedoch davon ausgegangen, dass Verletzungen der nach diesen Übereinkünften begründeten Rechte nach diesem Übereinkommen erst dann unter Strafe gestellt werden müssen, wenn diese Verträge für eine Vertragspartei in Kraft getreten sind.

112. Die Verpflichtung, Urheberrechtsverletzungen und Verletzungen verwandter Schutzrechte entsprechend den in völkerrechtlichen Übereinkünften eingegangenen Verpflichtungen unter Strafe zu stellen, erstreckt sich nicht auf nach den genannten Übereinkünften verliehene Urheberpersönlichkeitsrechte (wie in Artikel 6bis der Berner Übereinkunft und in Artikel 5 des WIPO-Urheberrechtsübereinkommens).

113. Straftaten in Bezug auf das Urheberrecht und verwandte Schutzrechte müssen „vorsätzlich“ begangen werden, um strafbar zu sein. Im Gegensatz zu allen übrigen materiell-rechtlichen Bestimmungen dieses Übereinkommens werden in Absatz 1 und in Absatz 2 im englischen Wortlaut der Ausdruck „wilfully“ und im französischen Wortlaut der Ausdruck „délibérément“ anstelle von „intentionally“ bzw. „intentionnellement“ gebraucht, da diese Ausdrücke im TRIPS-Übereinkommen (Artikel 61) verwendet werden, in welchem die Verpflichtung, Urheberrechtsverletzungen unter Strafe zu stellen, geregelt ist. *[Anm. d. Übers.: Im deutschen Wortlaut wird an allen Stellen der Ausdruck „vorsätzlich“ wie in der deutschen Fassung des TRIPS-Übereinkommens verwendet.]*

114. Mit diesen Bestimmungen sollen strafrechtliche Sanktionen für Verletzungen „in gewerbsmäßigem Umfang“ und mittels eines Computersystems vorgesehen werden. Dies entspricht Artikel 61 des TRIPS-Übereinkommens, nach dem strafrechtliche Sanktionen in Urheberrechtssachen nur bei „unerlaubter Herstellung ... in gewerbsmäßigem Umfang“ vorzusehen sind. Es kann jedoch sein, dass Vertragsparteien über die Schwelle „gewerbsmäßiger Umfang“ hinausgehen und auch Urheberrechtsverletzungen anderer Art unter Strafe stellen wollen.

115. Der Ausdruck „unbefugt“ ist im Wortlaut dieses Artikels überflüssig und ausgelassen worden, da der Ausdruck „Verletzung“ bereits bedeutet, dass urheberrechtlich geschütztes Material unbefugt benutzt wird. Dass der Ausdruck „unbefugt“ fehlt, schließt dagegen die Anwendung von Strafausschließungs- und Rechtfertigungsgründen sowie Grundsätzen über den Ausschluss strafrechtlicher Verantwortlichkeit in Verbindung mit dem Ausdruck „unbefugt“ an anderen Stellen im Übereinkommen nicht aus.

116. Absatz 3 erlaubt es den Vertragsparteien, unter „begrenzten Umständen“ (z. B. bei Parallelimporten, Vermietungsrechten) die Strafbarkeit nach den Absätzen 1 und 2 nicht zu begründen, sofern andere wirksame rechtliche Mittel einschließlich zivil- und/oder verwaltungsrechtlicher Maßnahmen zur Verfügung stehen. Im Wesentlichen befreit diese Bestimmung die Vertragsparteien in begrenzten Umfang von der Verpflichtung, die Strafbarkeit zu begründen, vorausgesetzt, sie weichen nicht von den Verpflichtungen nach Artikel 61 des TRIPS-Übereinkommens ab, welche die Mindestnorm im Bereich bereits bestehender Strafbarkeitsvorschriften darstellt.

117. Dieser Artikel darf keinesfalls so ausgelegt werden, als erstrecke sich der Schutz, der Urhebern, Filmproduzenten, ausübenden Künstlern, Herstellern von Tonträgern, Sendeunternehmen oder anderen Rechtsinhabern gewährt wird, auf Personen, die nach innerstaatlichem Recht oder einer internationalen Übereinkunft die Kriterien dafür nicht erfüllen.

Titel 5
Nebenformen der Verantwortlichkeit und Sanktionen

Versuch und Beihilfe oder Anstiftung (Artikel 11)

118. Der Zweck dieses Artikels ist, den Versuch oder die Teilnahme der in dem Übereinkommen beschriebenen Straftaten als Straftat festzulegen. Wie im Folgenden erläutert wird, braucht eine Vertragspartei nicht in Bezug auf jede in dem Übereinkommen festgelegte Straftat die Strafbarkeit des Versuchs vorzusehen.

119. Nach Absatz 1 haben die Vertragsparteien die Beteiligung an der Begehung von Straftaten nach den Artikeln 2 bis 10 als Straftat festzulegen. Die Beteiligung ist strafbar, wenn die Person, die eine im Übereinkommen definierte Straftat begeht, Hilfe von einer anderen Person erhält, die auch will, dass die Straftat begangen wird. So ist z. B. für die Übertragung von Daten mit schädlichem Inhalt oder von bösartigen Codes über das Internet zwar die Mitwirkung eines Diensteanbieters als Übermittler nötig, aber ein Diensteanbieter, bei dem ein strafrechtlicher Vorsatz nicht gegeben ist, kann sich nach dieser Bestimmung nicht strafbar machen. Ein Diensteanbieter ist also nicht verpflichtet, Inhalte aktiv zu überwachen, um eine strafrechtliche Verantwortlichkeit nach dieser Bestimmung zu vermeiden.

120. Im Hinblick auf den Versuch in Absatz 2 wurde bei einigen in dem Übereinkommen umschriebenen Straftaten oder Merkmalen dieser Straftaten der Versuch als begrifflich schwierig angesehen (z. B. der Tatbestand des Anbietens oder Verfügbarmachens von Kinderpornografie). In manchen Rechtsordnungen ist die Versuchsstrafbarkeit auf bestimmte Straftaten begrenzt. Dementsprechend wird nur verlangt, dass der Versuch in Bezug auf die nach den Artikeln 3, 4, 5, 7, 8 sowie 9 Absatz 1 Buchstabe a und c umschriebenen Straftaten mit Strafe bedroht wird.

121. Wie bei allen nach dem Übereinkommen festgelegten Straftaten ist Vorsatz auch Voraussetzung bei Versuch und Teilnahme.

122. Absatz 3 wurde hinzugefügt, um möglichen Schwierigkeiten der Vertragsparteien mit Absatz 2 zu begegnen, die sich in Anbetracht der weitgehend unterschiedlichen Begriffe in den verschiedenen Rechtsordnungen und trotz der Bemühungen in Absatz 2, bestimmte Aspekte von der Bestimmung über Versuch auszunehmen, ergeben können. Eine Vertragspartei kann erklären, dass sie sich das Recht vorbehält, Absatz 2 in seiner Gesamtheit oder in Teilen nicht anzuwenden. Dies bedeutet, dass eine Vertragspartei, die einen Vorbehalt zu dieser Bestimmung angebracht hat, nicht verpflichtet sein wird, den Versuch überhaupt unter Strafe zu stellen, oder dass sie die Straftaten oder Teile von Straftaten bestimmen kann, bei denen sie den Versuch unter Strafe stellt. Mit dem Vorbehalt soll erreicht werden, dass das Übereinkommen weitestgehend ratifiziert werden kann und den Vertragsparteien gleichzeitig erlaubt, einige ihrer grundlegenden Rechtsbegriffe beizubehalten.

Verantwortlichkeit juristischer Personen (Artikel 12)

123. Artikel 12 behandelt die Verantwortlichkeit juristischer Personen. Er entspricht der gegenwärtigen Rechtsentwicklung, juristischen Personen Verantwortlichkeit zuzuerkennen. Mit ihm soll Kapitalgesellschaften, Personenvereinigungen und ähnlichen juristischen Personen Verantwortlichkeit für strafbare Handlungen zuerkannt werden, die von einer Person in leitender Stellung innerhalb dieser juristischen Person und zum Vorteil für diese juristische Person begangen wurden. Artikel 12 sieht Verantwortlichkeit auch dann vor, wenn eine solche Person in Führungsposition es versäumt, einen Mitarbeiter oder Beauftragten der juristischen Person zu überwachen oder zu kontrollieren, soweit dieses Versäumnis die Begehung einer nach dem Übereinkommen festgelegten Straftat durch diesen Mitarbeiter oder Beauftragten ermöglicht.

124. Nach Absatz 1 müssen zur Begründung der Verantwortlichkeit vier Voraussetzungen erfüllt sein. Erstens muss eine der in dem Übereinkommen beschriebenen Straftaten begangen worden sein. Zweitens muss die Straftat zum Vorteil für die juristische Person begangen worden sein. Drittens muss eine Person in Führungsposition die Straftat (einschließlich des Versuchs) begangen haben. Der Ausdruck „Person, die eine Führungsposition innehat“ bezieht sich auf eine natürliche Person, die eine hohe Position in der Organisation bekleidet, z. B. den Geschäftsführer. Viertens muss die Person, die eine Führungsposition innehat, auf der Grundlage dieser Befugnisse gehandelt haben – Befugnis zur Vertretung der juristischen Person oder Befugnis, Entscheidungen zu treffen oder Kontrolle auszuüben –, die Beleg dafür sind, dass diese natürliche Person im Rahmen ihrer Befugnis gehandelt hat, so dass die juristische Person verantwortlich gemacht werden kann. Absatz 1 verpflichtet die Vertragsparteien im Ergebnis also, die Möglichkeit, eine juristische Person verantwortlich zu machen, nur in Bezug auf Straftaten vorzusehen, die von solchen Personen in Führungsposition begangen werden.

125. Darüber hinaus verpflichtet Absatz 2 die Vertragsparteien, die Möglichkeit, eine juristische Person verantwortlich zu machen, für den Fall vorzusehen, dass die Straftat nicht von der in Absatz 1 beschriebenen Person in Führungsposition, sondern von einer anderen im Auftrag der juristischen Person handelnden Person, d. h. einem ihrer im Rahmen seiner Befugnis handelnden Mitarbeiter oder Beauftragten, begangen wird. Die Voraussetzungen für die Zuerkennung der Verantwortlichkeit sind, (1) dass eine Straftat von einem solchen Mitarbeiter oder Beauftragten der juristischen Person begangen wurde, (2) dass die Straftat zum Vorteil für die juristische Person begangen wurde und (3) dass die Begehung der Straftat durch die mangelnde Überwachung des Mitarbeiters oder Beauftragten durch die Person in Führungsposition ermöglicht wurde. In diesem Zusammenhang ist unter mangelnder Überwachung auch zu verstehen, dass unterlassen wird, geeignete und angemessene Maßnahmen zu treffen, um Mitarbeiter oder Beauftragte daran zu hindern, strafbare Handlungen für die juristische Person zu begehen. Geeignete und angemessene Maßnahmen können von verschiedenen Faktoren bestimmt werden, so z. B. Art des Unternehmens, seine Größe, Standards oder eingeführte Geschäftspraktiken usw. Dies ist nicht so auszulegen, als würde eine allgemeine Überwachung der Kommunikationen der Mitarbeiter verlangt (siehe auch Nr. 54). Ein Diensteanbieter kann deshalb nicht aufgrund der Tatsache verantwortlich gemacht werden, dass in seinem System von einem Kunden, einem Nutzer oder einem anderen Dritten eine Straftat begangen wurde, weil der Ausdruck „in ihrem Auftrag handelnde“ ausschließlich auf Mitarbeiter und Beauftragte zutrifft, die im Rahmen ihrer Befugnis handeln.

126. Die Verantwortlichkeit nach diesem Artikel kann straf-, zivil- oder verwaltungsrechtlicher Art sein. Jeder Vertragspartei steht es frei, nach Maßgabe ihrer jeweiligen Rechtsgrundsätze zu entscheiden, ob sie alle diese Arten der Verantwortlichkeit oder einen Teil davon vorsieht, solange sie die Vorgaben des Artikels 13 Absatz 2 erfüllt, nach denen die Sanktion oder Maßnahme „wirksam, angemessen und abschreckend“ sein und Geldsanktionen einschließen muss.

127. Absatz 4 stellt klar, dass die Verantwortlichkeit juristischer Personen die individuelle Verantwortlichkeit nicht ausschließt.

Sanktionen und Maßnahmen (Artikel 13)

128. Dieser Artikel steht in engem Zusammenhang mit den Artikeln 2 bis 11, in denen verschiedene Computerstraftaten definiert sind, die mit strafrechtlichen Sanktionen bedroht werden sollen. Entsprechend den Verpflichtungen, die aus diesen Artikeln erwachsen, verpflichtet diese Bestimmung die Vertragsparteien, aus der Schwere dieser Straftaten Konsequenzen zu ziehen und strafrechtliche Sanktionen vorzusehen, die „wirksam, verhältnismäßig und abschreckend“ sind und bei natürlichen Personen die Möglichkeit der Verhängung von Freiheitsstrafen einschließen.

129. Juristische Personen, deren Verantwortlichkeit nach Artikel 12 zu begründen ist, können ebenfalls mit „wirksamen, verhältnismäßig und abschreckenden“ Sanktionen bedroht werden, die straf-, zivil- oder verwaltungsrechtlicher Art sein können. Die Vertragsparteien sind nach Absatz 2 verpflichtet, vorzusehen, dass gegen juristische Personen Geldsanktionen verhängt werden können.

130. Der Artikel lässt die Möglichkeit anderer der Schwere der Straftat entsprechender Sanktionen oder Maßnahmen offen; Maßnahmen könnten z. B. einstweilige Maßnahmen oder Einziehung umfassen. Er stellt es in das Ermessen der Vertragsparteien, ein System von Straftaten und Sanktionen zu schaffen, das mit ihren bestehenden innerstaatlichen Rechtsordnungen vereinbar ist.

Abschnitt 2 – Verfahrensrecht

131. Die Artikel in diesem Abschnitt beschreiben bestimmte verfahrensrechtliche Maßnahmen auf nationaler Ebene für die Zwecke strafrechtlicher Ermittlungen wegen der in Abschnitt 1 beschriebenen Straftaten und anderer mittels eines Computersystems begangener Straftaten und der Erhebung in elektronischer Form vorhandener Beweise für eine Straftat. Nach Artikel 39 Absatz 3 wird in diesem Übereinkommen weder verlangt, dass die Vertragsparteien andere als die im Übereinkommen enthaltenen Befugnisse und Verfahren festlegen, noch wird dies ausgeschlossen.

132. Die technologische Revolution einschließlich der „elektronischen Autobahn“, bei der zahlreiche Kommunikations- und Dienstleistungsformen durch gemeinsam genutzte Übertragungsmedien und Datenträger miteinander zusammenhängen und verbunden sind, hat den Bereich des Straf- und Strafverfahrensrechts verändert. Das sich ständig ausweitende Kommunikationsnetz öffnet neue Türen für die Kriminalität sowohl bei den traditionellen Straftaten als auch bei neuen technologischen Delikten. Nicht nur das materielle Strafrecht, sondern auch das Verfahrensrecht und die Ermittlungsmethoden müssen mit diesem neuen Missbrauch Schritt halten. Ebenso müssen Garantien angepasst oder entwickelt werden, die mit einer neuen technologischen Umwelt und neuen verfahrensrechtlichen Befugnissen Schritt halten können.

133. Eine der größten Herausforderungen bei der Verbrechensbekämpfung in der vernetzten Umwelt besteht in der Schwierigkeit, den Täter festzumachen und Ausmaß und Wirkung der kriminellen Handlung zu erkennen. Ein weiteres Problem ist die Flüchtigkeit der elektronischen Daten, die in Sekunden verändert, bewegt oder gelöscht werden können. Zum Beispiel kann ein Benutzer, der über die Daten verfügt, das Computersystem dazu benutzen, Daten, die Gegenstand von strafrechtlichen Ermittlungen sind, zu löschen und so Beweismittel zu vernichten. Schnelligkeit und zuweilen auch Geheimhaltung sind häufig entscheidend für den Erfolg von Ermittlungen.

134. Mit dem Übereinkommen werden traditionelle Ermittlungsmethoden wie Durchsuchung und Beschlagnahme an die neue technologische Umwelt angepasst. Daneben sind neue Maßnahmen geschaffen worden wie die beschleunigte Sicherung von Daten, damit sichergestellt ist, dass traditionelle Methoden der Beweissicherung wie Durchsuchung und Beschlagnahme auch in der flüchtigen technologischen Umwelt wirksam bleiben. Da Daten in der neuen technologischen Umwelt nicht immer statisch sind, sondern während der Übertragung fließend sein können, sind auch andere traditionelle, für die Telekommunikation relevante Erhebungsmethoden wie Echtzeiterhebung von Verkehrsdaten und Inhaltsdaten angepasst worden, damit im Übertragungsprozess befindliche Daten erfasst werden können. Einige dieser Maßnahmen sind in der Europaratsempfehlung Nr. R (95) 13 über Probleme des Strafverfahrensrechts im Zusammenhang mit Informationstechnologie dargestellt.

135. Alle in diesem Abschnitt enthaltenen Bestimmungen sind darauf gerichtet, die Beschaffung oder Erfassung von Daten zum Zweck besonderer strafrechtlicher Ermittlungen oder Verfahren zu ermöglichen. Die Verfasser des Übereinkommens haben erörtert, ob das Übereinkommen Diensteanbieter verpflichten soll, routinemäßig Verkehrsdaten zu erfassen und für eine bestimmte Zeit zu erhalten, haben jedoch mangels Einvernehmens keine derartige Verpflichtung aufgenommen.

136. Die Verfahren beziehen sich im Allgemeinen auf alle Arten von Daten, einschließlich der drei verschiedenen Arten von Computerdaten (Verkehrsdaten, Inhaltsdaten und Kundendaten), die in zweierlei Form vorhanden sein können (gespeichert oder im Übertragungsprozess befindlich). Definitionen einiger dieser Begriffe sind in den Artikeln 1 und 18 enthalten. Die Anwendbarkeit eines Verfahrens auf eine bestimmte Art oder Form elektronischer Daten hängt von der Art und Form der Daten und der Art des Verfahrens ab, wie in jedem Artikel gesondert beschrieben.

137. Bei der Anpassung traditioneller Verfahrensvorschriften an die neue technologische Umwelt stellt sich in den Bestimmungen dieses Abschnitts die Frage der geeigneten Terminologie. Zur Wahl standen die Beibehaltung der traditionellen Begriffe („durchsuchen“ und „beschlagnahmen“), die Verwendung neuer und mehr technologisch ausgerichteter Computerbegriffe („Zugriff“

und „Kopie“) wie in diesbezüglichen Texten anderer internationaler Foren (wie z. B. der G8-Untergruppe „High Tech Crime“) oder die Kompromisslösung einer gemischten Terminologie („Durchsuchung oder ähnlicher Zugriff“ und „beschlagnahmen oder in ähnlicher Weise sicherstellen“). Da die Entwicklung der Begriffe in der elektronischen Umwelt zum Ausdruck kommen soll und auch ihre traditionellen Wurzeln erkannt und erhalten werden sollen, wurde der flexible Ansatz gewählt, der es den Staaten erlaubt, die alten Begriffe „Durchsuchung und Beschlagnahme“ oder die neuen Begriffe „Zugriff und Kopieren“ zu verwenden.

138. Alle Artikel dieses Abschnitts nehmen Bezug auf die „zuständigen Behörden“ und die Befugnisse, die diesen zum Zweck besonderer strafrechtlicher Ermittlungen oder Verfahren erteilt werden. In einigen Ländern sind nur Richter befugt, das Sammeln oder die Herausgabe von Beweismitteln anzuordnen oder zu genehmigen, während in anderen Ländern Staatsanwälte oder andere Strafverfolgungsbeamte mit diesen oder ähnlichen Befugnissen ausgestattet sind. „Zuständige Behörde“ bezieht sich daher auf eine Justiz-, Verwaltungs- oder sonstige Strafverfolgungsbehörde, die nach innerstaatlichem Recht befugt ist, die Durchführung verfahrensrechtlicher Maßnahmen zum Zweck des Sammelns oder der Herausgabe von Beweismaterial bei bestimmten strafrechtlichen Ermittlungen oder Verfahren anzuordnen, zu genehmigen oder vorzunehmen.

Titel 1
Allgemeine Bestimmungen

139. Der Abschnitt beginnt mit zwei Bestimmungen allgemeiner Art, die sich auf alle das Verfahrensrecht betreffenden Artikel beziehen.

Geltungsbereich verfahrensrechtlicher Bestimmungen (Artikel 14)

140. Jede Vertragspartei ist verpflichtet, in Übereinstimmung mit ihrem innerstaatlichen Recht und rechtlichen Rahmenbedingungen die erforderlichen gesetzgeberischen und anderen Maßnahmen zu ergreifen, um die in diesem Abschnitt für die Zwecke „spezifischer strafrechtlicher Ermittlungen oder Verfahren“ vorgesehenen Befugnisse und Verfahren festzulegen.

141. Abgesehen von zwei Ausnahmen wird jede Vertragspartei die nach diesem Abschnitt festgelegten Befugnisse und Verfahren auf i) die nach Abschnitt 1 umschriebenen Straftaten, ii) andere mittels eines Computersystems begangene Straftaten und iii) die Erhebung von in elektronischer Form vorhandenen Beweisen für eine Straftat anwenden. Somit finden die Befugnisse und Verfahren nach diesem Abschnitt für die Zwecke spezifischer strafrechtlicher Ermittlungen und Verfahren auf die in Übereinstimmung mit dem Übereinkommen festgelegten Straftaten, andere mittels eines Computersystems begangene Straftaten und die Erhebung von in elektronischer Form vorhandenen Beweisen für eine Straftat Anwendung. Damit ist sichergestellt, dass in elektronischer Form vorhandene Beweise mittels der in diesem Abschnitt genannten Befugnisse und Verfahren beschafft oder gesammelt werden können. Dies schafft eine gleichwertige oder parallele Möglichkeit des Beschaffens oder Erfassens von Computerdaten, wie sie mit traditionellen Befugnissen und Verfahren für nicht elektronische Daten besteht.

Das Übereinkommen besagt, dass die Vertragsparteien in ihrem jeweiligen Recht die Möglichkeit vorsehen sollen, dass Informationen, die in digitaler oder sonstiger elektronischer Form vorhanden sind, im Strafverfahren als Beweismittel vor Gericht verwendet werden können, und zwar unabhängig von der Art der dem Verfahren zugrunde liegenden Straftat.

142. Von diesem Anwendungsbereich gibt es zwei Ausnahmen. Erstens sieht Artikel 21 vor, dass die Befugnis zur Erhebung von Inhaltsdaten auf nach dem innerstaatlichen Recht zu bestimmende schwere Straftaten begrenzt wird. Viele Staaten begrenzen die Befugnis zum Abfangen von mündlicher Kommunikation oder von Telekommunikation in Anbetracht der hier betroffenen Privatsphäre und die Verletzung der Privatsphäre durch diese Ermittlungsmethode auf einige schwere Straftaten. Ebenso verlangt das Übereinkommen lediglich, dass die Vertragsparteien Erhebungsbefugnisse und -verfahren in Bezug auf Inhaltsdaten bestimmter Kommunikationen mittels Computer bei einigen nach innerstaatlichen Recht zu bestimmenden schweren Straftaten festlegen.

143. Zweitens kann sich eine Vertragspartei das Recht vorbehalten, die Maßnahmen nach Artikel 20 (Erhebung von Verkehrsdaten in Echtzeit) nur auf in dem Vorbehalt genannte Straftaten oder Kategorien von Straftaten anzuwenden, wobei diese Straftaten oder Kategorien von Straftaten nicht stärker eingegrenzt sein dürfen als diejenigen, auf die die Erhebungsmaßnahmen nach Artikel 21 angewendet werden. Einige Staaten betrachten die Erhebung von Verkehrsdaten hinsichtlich der Privatsphäre und deren Verletzung als gleichbedeutend mit der Erhebung von Inhaltsdaten. Das Recht auf einen Vorbehalt erlaubt es diesen Staaten, die Anwendung der Maßnahmen zur Echtzeit-Erhebung von Verkehrsdaten auf die gleichen Straftaten zu begrenzen, auf die sie die Befugnisse und Verfahren für die Echtzeit-Erhebung von Inhaltsdaten anwenden. Viele Staaten betrachten jedoch die Erhebung von Inhaltsdaten und die Erhebung von Verkehrsdaten nicht als gleichbedeutend hinsichtlich der Privatsphäre und deren Verletzung, da die Erhebung nur der Verkehrsdaten nicht den Inhalt der Kommunikation erfasst oder offenbart. Da die Echtzeit-Erhebung von Verkehrsdaten für das Aufspüren der Quelle oder des Ziels von Computerkommunikation (somit für das Auffinden der Täter) sehr wichtig sein kann, werden die Vertragsparteien, die das Recht auf einen Vorbehalt wahrnehmen, im Übereinkommen aufgefordert, ihren Vorbehalt in dem Sinn zu beschränken, dass eine weitestgehende Anwendung der für die Echtzeit-Erhebung von Verkehrsdaten vorgesehenen Befugnisse und Verfahren ermöglicht wird.

144. In Buchstabe b ist ein Vorbehalt für Länder vorgesehen, die aufgrund von Beschränkungen in ihrem innerstaatlichen Recht, die im Zeitpunkt der Annahme des Übereinkommens gelten, Kommunikationen in Computersystemen, die für eine geschlossene Nutzergruppe betrieben werden und die sich keiner öffentlichen Kommunikationsnetze bedienen und auch nicht mit anderen Computersystemen verbunden sind, nicht erheben können. Der Ausdruck „geschlossene Nutzergruppe“ bezieht sich z. B. auf einen Nutzerkreis, der durch Anbindung an den Diensteanbieter begrenzt ist, wie die Mitarbeiter eines Unternehmens, denen das Unternehmen die Möglichkeit bietet, unter Benutzung eines Computernetzes miteinander zu kommunizieren. Der Ausdruck „nicht mit

anderen Computersystemen verbunden“ bedeutet, dass das System, in welchem Kommunikationen übertragen werden, in dem Zeitpunkt, in dem eine Anordnung nach Artikel 20 oder 21 ergehen würde, keine physische oder logische Verbindung zu einem anderen Computernetz hat. Der Ausdruck „sich keiner öffentlichen Kommunikationsnetze bedient“ schließt Systeme aus, die bei der Kommunikationsübertragung öffentliche Computernetze (einschließlich des Internets), öffentliche Telefonnetze oder andere öffentliche Telekommunikationseinrichtungen benutzen, gleichviel, ob diese Benutzung für den Nutzer erkennbar ist.

Bedingungen und Garantien (Artikel 15)

145. Die Schaffung, Umsetzung und Anwendung der in diesem Abschnitt des Übereinkommens vorgesehenen Befugnisse und Verfahren unterliegen den Bedingungen und Garantien nach dem innerstaatlichen Recht jeder Vertragspartei. Zwar sind die Vertragsparteien verpflichtet, bestimmte verfahrensrechtliche Bestimmungen in ihr innerstaatliches Recht aufzunehmen, jedoch unterliegen die Modalitäten der Schaffung und Umsetzung dieser Befugnisse und Verfahren in ihrem jeweiligen Rechtssystem und die Anwendung der Befugnisse und Verfahren in bestimmten Fällen dem innerstaatlichen Recht einer jeden Vertragspartei. Diese innerstaatlichen Rechtsvorschriften und Verfahren, die noch genauer beschrieben werden, umfassen Bedingungen und Garantien, die verfassungsrechtlich, gesetzlich, gerichtlich oder auf andere Weise begründet sein können. Zu den Modalitäten gehört, dass bestimmte Elemente als Bedingungen oder Garantien hinzugefügt werden, die einen Ausgleich schaffen zwischen den Erfordernissen der Strafverfolgung und dem Schutz der Menschenrechte und Freiheiten. Da das Übereinkommen für Vertragsparteien mit vielen unterschiedlichen Rechtssystemen und -kulturen gilt, ist es nicht möglich, die anwendbaren Bedingungen und Garantien für jede Befugnis und jedes Verfahren im Einzelnen darzulegen. Die Vertragsparteien müssen sicherstellen, dass diese Bedingungen und Garantien einen angemessenen Schutz der Menschenrechte und Freiheiten vorsehen. Es gibt einige allgemeine Standards oder Mindestgarantien, welche die Vertragsparteien des Übereinkommens erfüllen müssen. Dazu gehören Standards oder Mindestgarantien, die sich aus Verpflichtungen ergeben, die eine Vertragspartei nach internationalen Übereinkünften über Menschenrechte eingegangen ist. Zu diesen Übereinkünften gehören die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten von 1950 und deren Zusatzprotokolle Nr. 1, 4, 6, 7 und 12 (ETS Nr. 005[4]), 009, 046, 114, 117 und 177) im Hinblick auf die europäischen Vertragsstaaten dieser Übereinkünfte. Dazu gehören ferner andere Menschenrechtsübereinkünfte im Hinblick auf Staaten in anderen Regionen der Welt (z. B. die amerikanische Menschenrechtskonvention von 1969 und die afrikanische Charta der Menschenrechte und Rechte der Völker), die Vertragsparteien dieser Übereinkünfte sind, sowie der universell ratifizierte Internationale Pakt über bürgerliche und politische Rechte von 1966. Daneben gibt es ähnliche Schutzbestimmungen in den Gesetzen der meisten Staaten.

146. Eine weitere Garantie im Übereinkommen besteht darin, dass zu den Befugnissen und Verfahren „der Grundsatz der Verhältnismäßigkeit gehören muss“. Die Verhältnismäßigkeit wird von jeder Vertragspartei in Übereinstimmung mit den einschlägigen Grundsätzen ihres innerstaatlichen Rechts gewährleistet. Für die europäischen Länder ergibt sich aus den Grundsätzen der Europaratskonvention zum Schutz der Menschenrechte und Grundfreiheiten von 1950, aus der diesbezüglichen Rechtsprechung und aus der innerstaatlichen Gesetzgebung und Rechtsprechung, dass Befugnisse und Verfahren im angemessenen Verhältnis zur Art und zu den Umständen der Tat stehen müssen. Andere Staaten werden entsprechende Grundsätze ihres Rechts anwenden, so der Grundsatz, dass Herausgabeanordnungen nicht zu breit angelegt sein dürfen und Durchsuchungs- und Beschlagnahmemaßnahmen angemessen sein müssen. Auch die ausdrückliche Einschränkung in Artikel 21, wonach die Verpflichtungen hinsichtlich der Abfangmaßnahmen für eine Reihe nach dem innerstaatlichen Recht zu bestimmender schwerer Straftaten gelten, ist ein deutliches Beispiel für die Anwendung des Grundsatzes der Verhältnismäßigkeit.

147. Ohne die Art der anwendbaren Bedingungen und Garantien einzuschränken, verlangt das Übereinkommen insbesondere, dass diese Bedingungen und Garantien je nach Art der Befugnisse oder Verfahren eine richterliche oder sonstige unabhängige Kontrolle, die Begründung der Anwendung der Verfahren und die Begrenzung ihres Umfangs oder ihrer Dauer einschließen. Es ist im innerstaatlichen Recht in Anwendung verbindlicher internationaler Verpflichtungen und bestehender innerstaatlicher Grundsätze festzulegen, welche Befugnisse und Verfahren einschneidend genug sind, um die Anwendung besonderer Bedingung und Garantien erforderlich zu machen. Wie in Nr. 215 ausgeführt, sollen die Vertragsparteien beim Abfangen wegen des eingreifenden Charakters dieser Maßnahme derartige Bedingungen und Garantien anwenden. Andererseits brauchen derartige Garantien nicht unbedingt zum Beispiel bei der Datensicherung Anwendung finden. Weitere Garantien, die im innerstaatlichen Recht zu regeln wären, sind z. B. das Zeugnisverweigerungsrecht, Aussageverweigerungsrechte und Besonderheiten bei Personen oder Orten, die Gegenstand der Maßnahme sind.

148. Hinsichtlich der in Absatz 3 behandelten Angelegenheiten ist das „öffentliche Interesse“ von vorrangiger Bedeutung, insbesondere die Belange der „geordneten Rechtspflege“. Soweit es mit dem öffentlichen Interesse vereinbar ist, sollen die Vertragsparteien weitere, sich aus Vollstreckungsmaßnahmen ergebenden Faktoren wie die Auswirkungen der Befugnisse und Verfahren auf „die Rechte, Verantwortlichkeiten und berechtigten Interessen Dritter, einschließlich der Diensteanbieter“, berücksichtigen und prüfen, ob geeignete Maßnahmen zur Milderung dieser Auswirkungen ergriffen werden können. Zunächst werden also die geordnete Rechtspflege und andere öffentliche Interessen (z. B. öffentliche Sicherheit und öffentliches Gesundheitswesen sowie andere Belange einschließlich der Belange von Opfern und die Achtung der Privatsphäre) berücksichtigt. Soweit mit dem öffentlichen Interesse vereinbar, sind normalerweise auch Fragen wie möglichst geringe Störung der Verbraucherdienste, Schutz vor der Haftung für die Weitergabe oder die Erleichterung der Weitergabe nach diesem Kapitel oder Schutz von Eigentumsrechten zu berücksichtigen.

Titel 2
Umgehende Sicherung gespeicherter Computerdaten

149. Die Maßnahmen in Artikel 16 und 17 betreffen gespeicherte Daten, die von Dateninhabern wie Diensteanbietern bereits erhoben und erhalten wurden. Sie beziehen sich nicht auf die Echtzeit-Erhebung und Erhaltung künftiger Verkehrsdaten oder die Echtzeit-Erhebung auf den Inhalt von Übertragungen. Diese Fragen behandelt Titel 5.

150. Die in diesen Artikeln beschriebenen Maßnahmen greifen nur, wenn Computerdaten bereits existieren und gespeichert sind. Für strafrechtliche Ermittlungen relevante Computerdaten können aus vielerlei Gründen nicht existieren oder nicht mehr gespeichert sein. Es können zum Beispiel nicht die richtigen Daten erfasst oder erhalten, oder falls sie erfasst wurden, nicht aufrechterhalten worden sein. Datenschutzvorschriften können die Löschung wichtiger Daten verlangen, bevor überhaupt jemand ihre Bedeutung für ein Strafverfahren erkannt hat. Manchmal gibt es vielleicht keine betriebswirtschaftlichen Gründe für die Erfassung und Erhaltung von Daten, z. B. wenn die Kunden eine Pauschale für Dienste zahlen oder Dienste kostenlos sind. Die Artikel 16 und 17 behandeln diese Probleme nicht.

151. „Datensicherung“ ist von „Datenerhaltung“ zu unterscheiden. Während diese Begriffe allgemeinsprachlich eine ähnliche Bedeutung haben, sind sie im Computerbereich von unterschiedlicher Bedeutung. Daten sichern bedeutet, Daten, die bereits gespeichert sind, gegen alles zu schützen, was ihre gegenwärtige Eigenschaft oder Beschaffenheit verändern oder verschlechtern würde. Daten erhalten bedeutet, Daten, die gerade erzeugt werden, auch für die Zukunft in Besitz zu halten. Datenerhaltung bezeichnet die Ansammlung von Daten in der Gegenwart und ihr Besitz in die Zukunft hinein. Datenerhaltung ist der Prozess der Datenspeicherung. Datensicherung ist dagegen der Vorgang, mit dem gespeicherte Daten gesichert werden.

152. Die Artikel 16 und 17 beziehen sich nur auf die Datensicherung und nicht auf die Datenerhaltung. Sie betreffen nicht die Erhebung und Erhaltung aller oder auch nur einiger von einem Diensteanbieter oder einer anderen Stelle im Laufe ihrer Tätigkeiten erhobenen Daten. Die Sicherungsmaßnahmen gelten für Computerdaten, die „mittels eines Computersystems gespeichert wurden“, was voraussetzt, dass die Daten bereits existieren und erfasst und gespeichert sind. Außerdem sind nach Artikel 14 alle nach Abschnitt 2 des Übereinkommens festzulegenden Befugnisse und Verfahren „für die Zwecke spezifischer strafrechtlicher Ermittlungen oder Verfahren“ bestimmt, was die Anwendung der Maßnahmen auf die Ermittlungen in einem bestimmten Fall begrenzt. Außerdem bezieht sich die Anordnung, die eine Vertragspartei zur Anwendung von Sicherungsmaßnahmen trifft, auf „bestimmte gespeicherte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden“ (Absatz 2). Die Artikel begründen also nur die Befugnis, die Sicherung existierender gespeicherter Daten bis zu einer späteren Weitergabe der Daten aufgrund anderer gesetzlicher Befugnisse zu verlangen, und zwar im Zusammenhang mit spezifischen strafrechtlichen Ermittlungen oder Verfahren.

153. Die Verpflichtung zur Sicherung von Daten bedeutet nicht, dass die Vertragsparteien das Angebot oder die Nutzung von Diensten einschränken sollen, die nicht routinemäßig bestimmte Arten von Daten, wie z. B. Verkehrs- oder Kundendaten, im Rahmen ihrer rechtmäßigen Geschäftspraktiken erheben und erhalten. Es wird auch nicht verlangt, dass neue technische Möglichkeiten geschaffen werden, um dies tun zu können, z. B. um flüchtige Daten zu sichern, die nur so kurz im System vorhanden sind, dass sie kaum auf ein Ersuchen oder eine Anordnung hin gesichert werden können.

154. Einige Staaten haben Gesetze, wonach bestimmte Arten von Daten, so z. B. personenbezogene Daten, die im Besitz von bestimmten Inhabern sind, nicht erhalten werden dürfen und gelöscht werden müssen, sobald kein betriebswirtschaftlicher Grund mehr für die Erhaltung der Daten besteht. In der Europäischen Union ist der allgemeine Grundsatz in der Richtlinie 95/46/EG niedergelegt und im besonderen Kontext der Telekommunikation in der Richtlinie 97/66/EG. Diese Richtlinien begründen die Verpflichtung, Daten zu löschen, sobald ihre Speicherung nicht mehr notwendig ist. Die Mitgliedstaaten können jedoch Vorschriften erlassen, die Ausnahmen vorsehen, soweit dies zur Verhütung, Ermittlung und Verfolgung von Straftaten erforderlich ist. Diese Richtlinien hindern die Mitgliedstaaten der Europäischen Union nicht daran, in ihrem innerstaatlichen Recht Befugnisse und Verfahren zur Sicherung bestimmter Daten für spezifische Ermittlungen festzulegen.

155. Datensicherung ist für die meisten Länder eine völlig neue Befugnis oder Maßnahme im innerstaatlichen Recht. Sie ist eine wichtige neue Ermittlungshilfe im Bereich der Computerkriminalität, insbesondere bei Straftaten, die über das Internet begangen werden. Erstens können Computerdaten wegen ihrer Flüchtigkeit leicht manipuliert und verändert werden. Wertvolle Beweise für eine Straftat können leicht verloren gehen durch nachlässige Bearbeitungs- und Speicherpraktiken, durch vorsätzliche Manipulation oder Löschung, um Beweise zu vernichten, oder durch routinemäßige Löschung von Daten, die nicht mehr erhalten zu werden brauchen. Eine Methode der Sicherung der Datenintegrität besteht darin, dass die zuständigen Behörden eine Durchsuchung oder einen ähnlichen Zugriff vornehmen und die Daten beschlagnahmen oder in ähnlicher Weise sichern. Wenn jedoch der Verwahrer der Daten vertrauenswürdig ist, wie z. B. ein angesehenes Unternehmen, können die Daten mit einer Anordnung zur Datensicherung schneller sichergestellt werden. Bei rechtmäßiger Geschäftstätigkeit ist eine Sicherungsanordnung auch weniger störend für den normalen Geschäftsbetrieb und das Ansehen als die Durchführung von Durchsuchung und Beschlagnahme in den Geschäftsräumen. Zweitens werden Straftaten im Zusammenhang mit Computern weitgehend bei der Übertragung von Kommunikationen mittels Computersystemen begangen. Diese Kommunikationen können rechtswidrigen Inhalt wie z. B. Kinderpornografie enthalten, Computerviren oder Anleitungen, die einen Eingriff in Daten oder den ordnungsgemäßen Betrieb des Computersystems verursachen, oder Beweise für die Begehung anderer Straftaten wie Drogenhandel oder Betrug. Die Ermittlung der Quelle oder des Ziels dieser vergangenen Kommunikationen kann für die Feststellung der Identität der Täter hilfreich sein. Um diese Kommunikationen bis zu ihrer Quelle oder ihrem Ziel verfolgen zu können, werden die Verkehrsdaten betreffend diese Kommunikationen benötigt (siehe weitere Bemer-

kungen zur Bedeutung der Verkehrsdaten nachstehend zu Artikel 17). Drittens ist es wichtig, Kommunikationen zu sichern, die rechtswidrigen Inhalt oder Beweise für Straftaten enthalten und von denen Diensteanbieter Kopien, z. B. als E-Mail, besitzen, damit nicht entscheidende Beweise verloren gehen. Kopien vergangener Kommunikationen (z. B. gespeicherte E-Mail, die gesendet oder empfangen wurde) können Beweise für kriminelle Handlungen liefern.

156. Die Befugnis zur umgehenden Sicherung von Computerdaten soll diesen Problemen begegnen. Die Vertragsparteien sollen daher die Befugnis zur Anordnung der Sicherung bestimmter Computerdaten als vorläufige Maßnahme einführen, wonach Daten so lange wie notwendig für die Dauer von bis zu 90 Tagen gesichert werden. Eine Vertragspartei kann vorsehen, dass diese Anordnung anschließend verlängert werden kann. Das bedeutet nicht, dass die Daten im Zeitpunkt der Sicherung an Strafverfolgungsbehörden weitergegeben werden dürfen. Dazu bedarf es einer zusätzlichen Weitergabeanordnung oder eines Durchsuchungsbeschlusses. Zur Weitergabe gesicherter Daten an Strafverfolgungsbehörden siehe Nr. 152 und 160.

157. Wichtig ist auch, dass Sicherungsmaßnahmen auf nationaler Ebene bestehen, damit die Vertragsparteien einander auf internationaler Ebene mit der beschleunigten Sicherung von gespeicherten, in ihrem Hoheitsgebiet befindlichen Daten unterstützen können. Damit kann sichergestellt werden, dass bei den häufig zeitaufwändigen Verfahren der traditionellen Rechtshilfe, die es der ersuchten Vertragspartei ermöglichen, die Daten zu beschaffen und an die ersuchende Vertragspartei weiterzugeben, nicht wesentliche Daten verloren gehen.

Umgehende Sicherung gespeicherter Computerdaten (Artikel 16)

158. Mit Artikel 16 soll sichergestellt werden, dass die nationalen zuständigen Behörden die beschleunigte Sicherung bestimmter gespeicherter Computerdaten im Zusammenhang mit spezifischen strafrechtlichen Ermittlungen oder Verfahren anordnen oder auf ähnliche Weise erreichen können.

159. „Sicherung“ bedeutet, dass Daten, die bereits in gespeicherter Form existieren, gegen alles geschützt werden, was ihre gegenwärtige Eigenschaft oder Beschaffenheit verändern oder verschlechtern könnte. Dies bedeutet, dass die Daten gegen Änderung, Schädigung oder Löschung gesichert werden. Sicherung bedeutet nicht unbedingt, dass die Daten „eingefroren“ (d. h. unzugänglich gemacht) werden und die Daten oder Kopien davon nicht von rechtmäßigen Benutzern verwendet werden können. Die Person, an die die Anordnung gerichtet ist, kann immer noch, je nach den jeweiligen Anweisungen darin, auf die Daten zugreifen. Der Artikel schreibt nicht vor, wie die Daten zu sichern sind. Es bleibt jeder Vertragspartei überlassen zu bestimmen, auf welche Weise Daten gesichert werden und ob in geeigneten Fällen die Datensicherung auch das „Einfrieren“ einschließen soll.

160. Der Ausdruck „anordnen oder in ähnlicher Weise bewirken“ soll die Sicherung auch mit anderen rechtlichen Mitteln als einer gerichtlichen oder verwaltungsrechtlichen Anordnung oder Weisung (z. B. durch Polizei oder Staatsanwaltschaft) ermöglichen. Einige Staaten kennen in ihrem Verfahrensrecht keine Sicherungsanordnung und Daten können dort nur durch einen Durchsuchungs- und Beschlagnahmebeschluss oder eine Herausgabeanordnung gesichert und erlangt werden. Mit der Formulierung „in ähnlicher Weise bewirken“ soll Flexibilität erreicht werden, damit diese Staaten den Artikel mit diesen Mitteln umsetzen können. Es wird jedoch empfohlen, dass Staaten die Festlegung von Befugnissen und Verfahren prüfen, die den Empfänger einer Anordnung zur Datensicherung verpflichten, da schnelles Handeln dieser Person zu einer beschleunigten Anwendung der Sicherungsmaßnahmen im Einzelfall führen kann.

161. Die Befugnis, die beschleunigte Sicherung bestimmter Computerdaten anzuordnen oder in ähnlicher Weise zu bewirken, gilt für alle Arten gespeicherter Computerdaten. Dazu kann jede in der Anordnung bezeichnete Art von Daten gehören, so zum Beispiel Geschäfts-, Kranken-, Personal- oder andere Unterlagen. Die Vertragsparteien sollen Maßnahmen festlegen, „insbesondere wenn Gründe zu der Annahme bestehen, dass bei diesen Computerdaten eine besondere Gefahr des Verlusts oder der Veränderung besteht“. Dies kann der Fall sein, wo Daten über einen kurzen Zeitraum erhalten werden, wenn z. B. die Firmenpolitik darin besteht, Daten nach einer gewissen Zeit zu löschen, oder wo Daten gewöhnlich gelöscht werden, wenn das Speichermedium zur Aufzeichnung anderer Daten benötigt wird. Es kann auch mit dem Verwahrer der Daten zu tun haben oder mit der unsicheren Speicherung der Daten. Ist der Verwahrer nicht vertrauenswürdig, so wäre es jedoch sicherer, die Sicherung mit Durchsuchung und Beschlagnahme zu bewirken anstatt mit einer Anordnung, die nicht befolgt werden könnte. Die besondere Erwähnung der Verkehrsdaten in Absatz 1 soll deutlich machen, dass diese Vorschrift besonders auf diese Art von Daten anwendbar ist, die, wenn sie von einem Diensteanbieter erhoben und erhalten werden, gewöhnlich nur für kurze Zeit festgehalten werden. Die Erwähnung der Verkehrsdaten stellt auch einen Bezug zwischen den Maßnahmen in Artikel 16 und 17 her.

162. Absatz 2 besagt, dass, wenn eine Vertragspartei die Sicherung mit einer Anordnung an eine Person bewirkt, die Anordnung sich auf „bestimmte gespeicherte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden“ bezieht. Die gespeicherten Computerdaten können sich also tatsächlich im Besitz der Person befinden oder an einem anderen Ort gespeichert sein, jedoch der Verfügungsgewalt dieser Person unterliegen. Der Empfänger der Anordnung ist verpflichtet, „die Integrität der Computerdaten so lange wie notwendig für die Dauer von bis zu 90 Tagen zu sichern und zu erhalten, um den zuständigen Behörden zu ermöglichen, um deren Weitergabe zu ersuchen“. Das innerstaatliche Recht der Vertragsparteien sollte einen maximalen Zeitraum vorschreiben, über den einer Anordnung unterliegende Daten gesichert werden müssen, und in der Anordnung sollte genau angeben werden, über welchen Zeitraum die Daten zu sichern sind. Der Zeitraum soll so lang wie notwendig sein, maximal 90 Tage, um es den zuständigen Behörden zu gestatten, andere rechtliche Maßnahmen wie Durchsuchung und Beschlagnahme, andere Arten des Zugriffs oder der Sicherung oder eine Herausgabeanordnung zu ergreifen, um die Weitergabe der Daten zu erwirken. Eine Vertragspartei kann die

anschließende Verlängerung der Herausgabeanordnung vorsehen. In diesem Zusammenhang wird auf Artikel 29 verwiesen, der Rechthilfeersuchen zur Erwirkung der umgehenden Sicherung mittels Computersystemen gespeicherter Daten betrifft. Laut diesem Artikel erfolgt die Sicherung in Erledigung eines Rechtshilfeersuchens „für mindestens 60 Tage, damit die ersuchende Vertragspartei ein Ersuchen um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten stellen kann".

163. Absatz 3 verpflichtet den Verwahrer der zu sichernden Daten oder die mit der Sicherung betraute Person zur Vertraulichkeit in Bezug auf die Durchführung der Sicherungsverfahren über einen nach innerstaatlichem Recht vorgesehenen Zeitraum. Dies erfordert, dass die Vertragsparteien auf Vertraulichkeit gerichtete Maßnahmen im Hinblick auf die beschleunigte Sicherung gespeicherter Daten ergreifen und eine Frist für die Dauer der Vertraulichkeit festlegen. Diese Maßnahme dient den Zwecken der Strafverfolgung, damit der Verdächtige nicht von den Ermittlungen erfährt, wie auch dem Recht auf Privatsphäre. Für die Strafverfolgungsbehörden ist die beschleunigte Sicherung von Daten Teil der Anfangsermittlungen und daher kann die vertrauliche Behandlung in diesem Stadium von Bedeutung sein. Die Sicherung ist eine vorläufige Maßnahme bis zur Ergreifung anderer rechtlicher Maßnahmen zur Erlangung oder Weitergabe der Daten. Vertraulichkeit ist erforderlich, damit niemand anderes versucht, die Daten zu fälschen oder zu löschen. Für denjenigen, an den die Anordnung gerichtet ist, den die Daten betreffen oder der in den Daten erwähnt oder bezeichnet ist, gibt es eine eindeutige Frist für die Dauer der Maßnahme. Die doppelte Verpflichtung, die Daten zu sichern und Vertraulichkeit über die Tatsache der Sicherungsmaßnahme zu wahren, trägt dazu bei, die Privatsphäre des Betroffenen oder anderer in den Daten erwähnter oder bezeichneter Personen zu schützen.

164. Neben den oben beschriebenen Einschränkungen unterliegen die in Artikel 16 genannten Befugnisse und Verfahren den in den Artikeln 14 und 15 vorgesehenen Bedingungen und Garantien.

Umgehende Sicherung und teilweise Weitergabe von Verkehrsdaten (Artikel 17)

165. Dieser Artikel schafft besondere Verpflichtungen in Bezug auf die Sicherung von Verkehrsdaten nach Artikel 16 und sieht die beschleunigte Weitergabe einiger Verkehrsdaten vor, so dass festgestellt werden kann, dass noch weitere Diensteanbieter an der Übertragung bestimmter Kommunikationen beteiligt waren. „Verkehrsdaten" sind in Artikel 1 definiert.

166. Gespeicherte Verkehrsdaten zu erlangen, die mit vergangenen Kommunikationen zu tun haben, kann wichtig sein für die Feststellung der Quelle oder des Ziels einer vergangenen Kommunikation, was entscheidend ist für die Entdeckung von Personen, die z. B. Kinderpornografie verbreitet haben, betrügerisch falsche Angaben als Teil eines Betrugsplans verbreitet haben, Computerviren verbreitet haben, einen rechtswidrigen Zugriff auf Computersysteme versucht oder vollendet haben oder Kommunikationen an ein Computersystem übertragen haben, die in Daten in diesem System oder in den ordnungsgemäßen Betrieb dieses Systems eingegriffen haben. Diese Daten werden jedoch häufig nur kurzfristig gespeichert, da möglicherweise Gesetze zum Datenschutz oder Marktkräfte einer langfristigen Speicherung entgegenstehen. Daher ist es wichtig, dass Sicherungsmaßnahmen ergriffen werden, um die Integrität dieser Daten zu bewahren (siehe oben die Ausführungen zur Sicherung).

167. Häufig ist mehr als ein Diensteanbieter an der Übertragung einer Kommunikation beteiligt. Jeder Diensteanbieter besitzt vielleicht einige Verkehrsdaten der Übertragung einer bestimmten Kommunikation, die entweder von diesem Diensteanbieter mit der Passage der Kommunikation durch sein System erzeugt und erhalten wurden oder von anderen Diensteanbietern geliefert wurden. Manchmal werden Verkehrsdaten oder zumindest einige Arten von Verkehrsdaten zwischen den an einer Übertragung beteiligten Diensteanbietern aus geschäftlichen, Sicherheits- oder technischen Gründen geteilt. In solch einem Fall kann irgendeiner der Diensteanbieter die wesentlichen Daten besitzen, die zur Feststellung der Quelle oder des Ziels der Kommunikation benötigt werden. Häufig besitzt jedoch kein einzelner Diensteanbieter genügend Verkehrsdaten, die es ermöglichen würden, die tatsächliche Quelle oder das Ziel der Kommunikation zu erkennen. Jeder besitzt ein Teilstück des Puzzle, und jedes Teilstück muss geprüft werden, damit die Quelle oder das Ziel erkennbar wird.

168. Haben ein oder mehrere Diensteanbieter an der Übertragung einer Kommunikation mitgewirkt, gewährleistet Artikel 17, dass bei allen Diensteanbietern eine umgehende Sicherung der Verkehrsdaten möglich ist. Der Artikel bestimmt nicht den Weg, auf dem dieses Ziel erreicht werden kann, und überlässt es dem innerstaatlichen Recht, ein Verfahren festzulegen, das mit seiner Rechts- und Wirtschaftsordnung im Einklang steht. Eine Methode zur beschleunigten Sicherung dürfte für die zuständigen Behörden in der umgehenden Zustellung einer gesonderten Sicherungsanordnung an jeden Diensteanbieter bestehen. Dennoch kann es übermäßig viel Zeit in Anspruch nehmen, eine Reihe gesonderter Anordnungen zu erwirken. Eine wünschenswerte Alternative könnte darin bestehen, eine einzige Anordnung zu erwirken, deren Geltung sich jedoch auf alle Diensteanbieter erstrecken würde, deren Mitwirkung an der Übertragung der bestimmten Kommunikation sich anschließend herausstellt. Diese Gesamtanordnung könnte jedem nachweislich beteiligten Diensteanbieter der Reihe nach zugestellt werden. Andere mögliche Alternativen könnten in der Beteiligung von Diensteanbietern bestehen. So könnte von einem Diensteanbieter, dem eine Anordnung zugestellt worden ist, verlangt werden, den Diensteanbieter, der das nächste Glied in der Kette darstellt, von der Sicherungsanordnung und deren Bedingungen zu unterrichten. Diese Unterrichtung könnte entsprechend dem innerstaatlichen Recht bewirken, dass dem anderen Diensteanbieter erlaubt wird, die maßgeblichen Verkehrsdaten trotz etwaiger Löschungsverpflichtungen freiwillig zu sichern, oder dass deren Sicherung angeordnet wird. Der folgende Diensteanbieter könnte den Diensteanbieter, der das nächste Glied in der Kette darstellt, in gleicher Weise in Kenntnis setzen.

169. Da Verkehrsdaten nicht aufgrund der Zustellung einer Sicherungsanordnung an einen Diensteanbieter an die Strafverfolgungsbehörden weitergegeben werden (sondern erst aufgrund weiterer rechtlicher Schritte erlangt oder weitergegeben werden), ist diesen Behörden

nicht bekannt, ob der Diensteanbieter alle entscheidenden Verkehrsdaten besitzt oder ob weitere Diensteanbieter an der Kommunikationsübertragungskette beteiligt sind. Daher schreibt dieser Artikel vor, dass der Diensteanbieter, der eine Sicherungsanordnung oder Ähnliches empfängt, eine hinreichende Menge Verkehrsdaten an die zuständigen Behörden oder an eine andere dafür vorgesehene Person umgehend weitergibt, um den zuständigen Behörden zu ermöglichen, andere Diensteanbieter und den Pfad, auf dem die Kommunikation übertragen wurde, zu identifizieren. Die zuständigen Behörden sollen die Art der weiterzugebenden Verkehrsdaten eindeutig angeben. Nach Eingang dieser Auskünfte dürften die zuständigen Behörden in der Lage sein zu entscheiden, ob im Hinblick auf die anderen Diensteanbieter Sicherungsanordnungen zu erlassen sind. Auf diese Weise können die Ermittlungsbehörden die Kommunikation bis zur Quelle zurückverfolgen oder an ihr Ziel weiterleiten und feststellen, wer die Straftat, derentwegen ermittelt wird, begangen hat. Die Maßnahmen dieses Artikels unterliegen auch den Beschränkungen, Bedingungen und Garantien nach Artikel 14 und 15.

Titel 3
Anordnung der Herausgabe

Anordnung der Herausgabe (Artikel 18)

170. Absatz 1 dieses Artikels fordert die Vertragsparteien auf, es ihren zuständigen Behörden zu ermöglichen, eine Person in ihrem Hoheitsgebiet zu zwingen, bestimmte gespeicherte Computerdaten vorzulegen, oder einen Diensteanbieter, der seine Dienste in ihrem Hoheitsgebiet anbietet, zu zwingen, Kundendaten vorzulegen. Die fraglichen Daten sind gespeicherte oder vorhandene Daten und schließen noch nicht erzeugte Daten wie Verkehrsdaten oder auf künftige Kommunikationen bezogene Inhaltsdaten nicht ein. Von den Staaten soll nicht verlangt werden, gegenüber Dritten systematisch Zwangsmaßnahmen wie Durchsuchung und Beschlagnahme von Daten anzuwenden; vielmehr sollen im jeweiligen innerstaatlichen Recht alternative Ermittlungsbefugnisse festgelegt werden, die ein weniger einschneidendes Verfahren zur Erlangung von Informationen im Zusammenhang mit strafrechtlichen Ermittlungen vorsehen.

171. Eine „Anordnung der Herausgabe“ stellt eine flexible Maßnahme dar, welche die Strafverfolgungsbehörden in vielen Fällen anwenden können, insbesondere anstelle von stärker eingreifenden oder belastenden Maßnahmen. Die Einführung eines solchen Verfahrens ist auch für Drittverwahrer von Daten von Vorteil, etwa für die ISPs, die oft bereit sind, den Strafverfolgungsbehörden bei der Beschaffung von Daten in ihrer Verfügungsgewalt behilflich zu sein, aber für diese Hilfe eine angemessene Rechtsgrundlage vorziehen, die sie von jeder vertraglichen oder außervertraglichen Haftung befreit.

172. Die Herausgabeanordnung bezieht sich auf Computerdaten oder Kundendaten, die sich im Besitz oder unter Kontrolle einer Person oder eines Diensteanbieters befinden. Die Maßnahme kann nur angewandt werden, wenn die Person oder der Diensteanbieter über solche Daten oder Informationen verfügt. Manche Diensteanbieter führen zum Beispiel keine Unterlagen über die Kunden ihrer Dienste.

173. Nach Absatz 1 Buchstabe a stellt eine Vertragspartei sicher, dass ihre zuständigen Strafverfolgungsbehörden befugt sind anzuordnen, dass eine Person in ihrem Hoheitsgebiet bestimmte Computerdaten, die in einem Computersystem oder auf einem Datenträger gespeichert sind und die sich in ihrem Besitz oder unter ihrer Kontrolle befinden, vorzulegen. Der Ausdruck „Besitz oder Kontrolle“ bezieht sich auf den physischen Besitz der betreffenden Daten im Hoheitsgebiet der anordnenden Vertragspartei und auf Situationen, in denen sich die herauszugebenden Daten nicht im physischen Besitz der betreffenden Person befinden, diese Person jedoch vom Hoheitsgebiet der anordnenden Vertragspartei aus die Herausgabe der Daten veranlassen kann (z. B. muss eine Person, der eine Herausgabeanordnung für Informationen zugestellt wird, die für sie mittels eines Online-Fernspeicherdienstes gespeichert sind, diese Informationen – vorbehaltlich anwendbarer Aussageverweigerungsrechte – herausgeben). Andererseits stellt die bloße technische Möglichkeit des Zugriffs auf ferngespeicherte Daten (z. B. die Möglichkeit für einen Benutzer, über eine Netzwerkverbindung auf ferngespeicherte Daten zuzugreifen, die nicht seiner rechtmäßigen Verfügungsgewalt unterliegen) nicht unbedingt „Kontrolle“ im Sinne dieser Vorschrift dar. In einigen Staaten umfasst der im Gesetz mit „Besitz“ bezeichnete Begriff den physischen und konstruktiven Besitz und kann weit genug ausgelegt werden, um dieser Voraussetzung „Besitz oder Kontrolle“ gerecht zu werden.

Nach Absatz 1 Buchstabe b sieht eine Vertragspartei auch die Befugnis vor, von einem Diensteanbieter, der seine Dienste in ihrem Hoheitsgebiet anbietet, zu verlangen, „Kundendaten, die sich in seinem Besitz oder seiner Verfügungsgewalt befinden, vorzulegen“. Wie in Buchstabe a bezieht sich der Ausdruck „Besitz oder Kontrolle“ auf Kundendaten im physischen Besitz des Diensteanbieters und auf ferngespeicherte Kundendaten in der Kontrolle des Diensteanbieters (z. B. in einem Datenfernspeicher eines anderen Unternehmens). Der Ausdruck „in Zusammenhang mit diesen Diensten“ bedeutet, dass die Befugnis gelten soll für die Herausgabe von Kundendaten in Zusammenhang mit Diensten, die im Hoheitsgebiet der anordnenden Vertragspartei angeboten werden.

174. Da die Bedingungen und Garantien nach Absatz 2 dieses Artikels von dem innerstaatlichen Recht jeder Vertragspartei abhängen, können sie bevorrechtigte Daten oder Informationen ausschließen. Eine Vertragspartei kann den Wunsch haben, für die Vorlage bestimmter Arten von Computer- oder Kundendaten, über die besondere Kategorien von Personen oder Diensteanbietern verfügen, andere Bedingungen, andere zuständige Stellen und andere Garantien vorzusehen. So kann eine Vertragspartei Strafverfolgungsbeamten im Hinblick auf bestimmte Datenarten wie öffentlich zugängliche Kundendaten gestatten, eine derartige Anordnung zu erlassen, während es unter anderen Umständen hierzu einer gerichtlichen Anordnung bedürfte. Andererseits kann eine Vertragspartei in einigen Fällen verlangen oder von Menschenrechtsgarantien geleitet sein zu verlangen, dass eine Herausgabeanordnung nur von den Gerichten erlassen werden kann, um bestimmte Datenarten erlangen zu können. Parteien können den Wunsch haben, die Weitergabe dieser Daten für Strafverfolgungszwecke auf Fälle zu beschränken, in denen eine Herausgabeanordnung zwecks Weitergabe solcher Daten von den Gerich-

ten erlassen worden ist. Der Grundsatz der Verhältnismäßigkeit gewährt auch eine gewisse Flexibilität bei der Anwendung dieser Maßnahme, die zum Beispiel in vielen Staaten in Bagatellsachen ausgeschlossen ist.

175. Die Parteien können auch erwägen, Geheimhaltungsmaßnahmen einzubeziehen. Die Bestimmung nimmt nicht ausdrücklich auf die Geheimhaltung Bezug, um die Vergleichbarkeit mit dem nichtelektronischen Bereich zu wahren, in dem Herausgabeanordnungen allgemein nicht der Geheimhaltung unterliegen. Auf dem Gebiet der Elektronik und insbesondere im Online-Bereich kann eine Herausgabeanordnung bisweilen als Maßnahme im Vorfeld eines Ermittlungsverfahrens eingesetzt werden, die weiteren Maßnahmen wie der Durchsuchung und Beschlagnahme oder der Echtzeit-Erhebung sonstiger Daten vorausgeht. Die Geheimhaltung könnte für den erfolgreichen Abschluss des Ermittlungsverfahrens ausschlaggebend sein.

176. Im Hinblick auf die Durchführung der Herausgabe könnten die Vertragsparteien Auflagen festlegen, nach denen die Computer- oder Kundendaten in der in der Anordnung bestimmten Weise herauszugeben sind. Dies könnte bedeuten, dass eine Frist, innerhalb derer die Weitergabe erfolgen muss, genannt wird oder eine Form wie „Klartext“, Online, Papierausdruck oder Diskette, in der die Daten oder Informationen vorzulegen sind, vorgeschrieben wird.

177. „Kundendaten“ werden in Absatz 3 definiert. Sie bedeuten grundsätzlich jede Information, über die der Administrator eines Diensteanbieters verfügt und die sich auf die Kunden seiner Dienste beziehen. Kundendaten können Informationen sein, die in Form von Computerdaten oder in anderer Form wie Schriftstücken vorliegen. Da Kundendaten auch andere Formen von Daten als Computerdaten enthalten, ist in diesen Artikel eine besondere Bestimmung aufgenommen worden, die sich auf diese Art von Daten bezieht. „Kunde“ soll einen großen Kreis von Nutzern des Diensteanbieters einschließen, von Beitragszahlern über diejenigen, die pro Nutzung zahlen, bis zu denen, die Dienste kostenlos in Anspruch nehmen. Eingeschlossen sind auch Daten zu Personen, die berechtigt sind, das Kundenkonto zu nutzen.

178. Im Laufe eines strafrechtlichen Ermittlungsverfahrens können Kundendaten in erster Linie in zwei bestimmten Fällen benötigt werden. Im ersten Fall werden Kundendaten benötigt, um festzustellen, welche Dienste und dazugehörige technische Einrichtungen von dem Kunden genutzt worden sind oder genutzt werden, so die Art des verwendeten Telefondienstes (z. B. Mobiltelefon), die Art anderer genutzter dazugehöriger Dienste (z. B. Rufumleitung, Voicemail usw.), Telefonnummern und andere technische Adressen (z. B. E-Mail-Adressen). Im zweiten Fall, wenn eine technische Anschrift bekannt ist, werden Kundendaten zur Feststellung der Identität des Betroffenen benötigt. Sonstige Kundendaten wie Geschäftsdaten über Rechnungsstellung und Zahlungsunterlagen des Kunden können auch für strafrechtliche Ermittlungen erheblich sein, insbesondere in den Fällen, in denen die zu untersuchende Straftat mit Computerbetrug oder anderen Wirtschaftsstraftaten zu tun hat.

179. Aus diesem Grund beinhalten Kundendaten verschiedene Arten von Informationen über die Nutzung eines Dienstes und den Nutzer dieses Dienstes. Im Hinblick auf die Nutzung des Dienstes bedeutet der Begriff Informationen, die keine Verkehrs- oder Inhaltsdaten darstellen und mittels derer die Art des genutzten Kommunikationsdienstes, die dazugehörigen technischen Maßnahmen und der Zeitraum, in dem der Kunde den Dienst in Anspruch genommen hat, festgestellt werden können. Der Begriff „technische Maßnahmen“ beinhaltet alle Maßnahmen, die getroffen werden, damit ein Kunde den angebotenen Kommunikationsdienst nutzen kann. Derartige Maßnahmen umfassen die Bereitstellung einer technischen Nummer oder Adresse (Telefonnummer, Website-Adresse oder Domäne-Name, E-Mail-Adresse usw.) sowie die Beschaffung und Registrierung der von dem Kunden genutzten Kommunikationsanlagen wie Fernmeldeeinrichtungen, Callcenter oder lokale Netzwerke.

180. Kundendaten beschränken sich nicht auf Informationen, die sich unmittelbar auf die Nutzung eines Kommunikationsdienstes beziehen. Sie bedeuten auch Informationen, mit Ausnahme von Verkehrsdaten oder Inhaltsdaten, mit denen die Identität des Nutzers, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage eines Vertrags oder einer Vereinbarung in Bezug auf den Dienst zur Verfügung stehen, festgestellt werden können. Sie bedeuten auch sonstige Informationen, mit Ausnahme von Verkehrsdaten oder Inhaltsdaten, über den Ort der Installation der Kommunikationsanlage, die auf der Grundlage eines Vertrags oder einer Vereinbarung in Bezug auf den Dienst zur Verfügung stehen. Diese Daten dürften in der Praxis nur bei nicht transportierbaren Anlagen von Bedeutung sein, aber Informationen über die Tragbarkeit oder den angeblichen Standort der Anlage (anhand der Angaben aus dem Vertrag oder der Vereinbarung in Bezug auf den Dienst) können einem Ermittlungsverfahren förderlich sein.

181. Dieser Artikel ist jedoch nicht so zu verstehen, als verpflichte er die Diensteanbieter, Unterlagen über ihre Kunden zu führen oder die Richtigkeit solcher Angaben zu gewährleisten. So ist ein Diensteanbieter nicht verpflichtet, personenbezogene Daten von Nutzern sogenannter Prepaid Cards für mobile Telefondienste zu registrieren. Er ist auch nicht verpflichtet, die Identität der Kunden zu überprüfen oder den Nutzern seiner Dienste die Verwendung von Pseudonymen zu verbieten.

182. Da die in diesem Abschnitt vorgesehenen Befugnisse und Verfahren für besondere spezifische Ermittlungen oder Verfahren festgelegt werden (Artikel 14), ist von Herausgabeanordnungen, die im Allgemeinen bestimmte Kunden betreffen, in Einzelfällen Gebrauch zu machen. So kann anhand eines bestimmten Namens, der in der Herausgabeanordnung genannt wird, die Angabe einer bestimmten dazugehörigen Telefonnummer oder E-Mail-Adresse verlangt werden. Auf der Grundlage einer bestimmten Telefonnummer oder E-Mail-Adresse kann die Angabe des Namens und der Anschrift des betreffenden Kunden verlangt werden. Die Bestimmung ermächtigt die Vertragsparteien nicht, z. B. zum Zweck des „data mining“ eine Anordnung auf Weitergabe beliebiger Mengen von Kundendaten eines Diensteanbieters, die sich auf bestimmte Kundengruppen beziehen, zu erlassen.

183. Die Bezugnahme auf „den Vertrag oder die Vereinbarung in Bezug auf den Dienst“ ist weit auszulegen und

beinhaltet jede Art von Beziehung, aufgrund derer ein Kunde die Dienste des Anbieters nutzt.

Titel 4
Durchsuchung und Beschlagnahme gespeicherter Computerdaten

Durchsuchung und Beschlagnahme gespeicherter Computerdaten (Artikel 19)

184. Dieser Artikel dient dazu, die innerstaatlichen Rechtsvorschriften über die Durchsuchung und Beschlagnahme gespeicherter Computerdaten zum Zweck der Erlangung von Beweismaterial für spezifische strafrechtliche Ermittlungen oder Verfahren zu modernisieren und zu vereinheitlichen. Jedes innerstaatliche Strafverfahrensrecht enthält Befugnisse zur Durchsuchung und zur Beschlagnahme körperlicher Gegenstände. In einigen Staaten gelten jedoch gespeicherte Computerdaten an sich nicht als körperliche Gegenstände und können daher nicht in gleicher Weise wie körperliche Gegenstände für strafrechtliche Ermittlungen und Verfahren sichergestellt werden, es sei denn durch Sicherstellung des Datenträgers, auf dem sie gespeichert sind. Mit Artikel 19 des Übereinkommens soll eine entsprechende Befugnis für gespeicherte Daten geschaffen werden.

185. Bei der Durchsuchung unter traditionellen Bedingungen, bei der es um Dokumente oder Aufzeichnungen geht, beinhaltet eine Durchsuchung das Sammeln von Beweismitteln, die in greifbarer Form, wie Tinte auf Papier, vorliegen. Die Ermittler durchsuchen oder prüfen die aufgezeichneten Daten; die greifbare Aufzeichnung wird beschlagnahmt oder physisch weggenommen. Das Sammeln der Daten findet im Verlauf der Durchsuchung statt und bezieht sich auf Daten, die zu diesem Zeitpunkt vorliegen. Voraussetzung der Erlangung der gesetzlichen Befugnis zur Vornahme einer Durchsuchung sind nach den innerstaatlichen Rechtsvorschriften und Menschenrechtsgarantien Anhaltspunkte dafür, dass solche Daten sich an einem bestimmten Ort befinden und bezüglich einer bestimmten Straftat als Beweismittel dienen können.

186. Was die Suche nach Beweismaterial, insbesondere Computerdaten, unter den neuen technologischen Bedingungen betrifft, so sind viele Merkmale der traditionellen Durchsuchung weiterhin gegeben. Zum Beispiel erfolgt das Sammeln von Daten im Verlauf der Durchsuchung und bezieht sich auf Daten, die zu diesem Zeitpunkt vorhanden sind. Die Voraussetzungen für die Erlangung der gesetzlichen Befugnis zur Vornahme einer Durchsuchung bleiben dieselben. Die Zuverlässigkeit der Annahme, die für den Erhalt einer gesetzlichen Befugnis zur Durchsuchung erforderlich ist, ist dieselbe, ob die Daten nun in greifbarer oder in elektronischer Form vorliegen. Ebenso beziehen sich die Anhaltspunkte und die Durchsuchung auf Daten, die bereits vorhanden sind und bezüglich einer bestimmten Straftat als Beweismittel dienen können.

187. Bezüglich der Durchsuchung von Computerdaten sind zusätzliche verfahrensrechtliche Bestimmungen erforderlich, damit gewährleistet ist, dass Computerdaten auf eine Weise erlangt werden können, die ebenso wirksam ist wie eine Durchsuchung und Beschlagnahme greifbarer Datenträger. Dafür gibt es mehrere Gründe: Erstens liegen die Daten in nicht greifbarer Form vor, beispielsweise in elektromagnetischer Form. Zweitens können die Daten zwar vielleicht mit Hilfe eines Computers gelesen, jedoch nicht in demselben Sinn beschlagnahmt werden, wie dies bei einer Papieraufzeichnung der Fall ist. Das physische Medium, auf dem die nicht greifbaren Daten gespeichert sind (d. h. die Computer-Festplatte oder eine Diskette) muss beschlagnahmt und mitgenommen werden, oder es muss eine Kopie der Daten entweder in greifbarer Form (z. B. Papierausdruck) oder nicht greifbarer Form auf einem Träger (z. B. Diskette) angefertigt werden, bevor das greifbare Medium, das die Kopie beinhaltet, beschlagnahmt und mitgenommen werden kann. In den beiden letztgenannten Fällen, in denen von den Daten eine solche Kopie angefertigt wird, verbleibt eine Kopie der Daten im Computersystem oder der Speichervorrichtung. Die Befugnis, solche Kopien anzufertigen, soll im innerstaatlichen Recht vorgesehen werden. Drittens kann es aufgrund der Vernetzbarkeit zwischen Computersystemen der Fall sein, dass Daten zwar nicht in dem bestimmten, durchsuchten Computer gespeichert, aber über das betreffende System leicht zugänglich sind. Sie könnten in einer Datenspeichervorrichtung gespeichert sein, die mit dem Computer entweder direkt oder indirekt über ein Kommunikationssystem wie das Internet verbunden ist. Dies macht es möglicherweise erforderlich, neue Rechtsvorschriften zu erlassen, die eine Ausweitung der Durchsuchung auf den Ort, an dem die Daten tatsächlich gespeichert sind (oder eine Rückführung der Daten von diesem Ort an den durchsuchten Computer), ermöglichen oder traditionelle Durchsuchungsbefugnisse in einer besser koordinierten und zügigeren Weise an beiden Orten zu nutzen.

188. Absatz 1 verpflichtet die Vertragsparteien, den Strafverfolgungsbehörden die Befugnis zu erteilen, auf Daten zuzugreifen und Daten zu durchsuchen, die sich in einem Computersystem oder einem Teil davon (wie z. B. einer verbundenen Datenspeichervorrichtung) oder auf einem unabhängigen Datenspeichermedium (wie einer CD-ROM oder Diskette) befinden. Da der Begriff „Computersystem“ in Artikel 1 als „eine Vorrichtung oder eine Gruppe verbundener oder zusammenhängender Vorrichtungen“ definiert ist, betrifft Absatz 1 die Durchsuchung eines Computersystems und der mit diesem zusammenhängenden Komponenten, die zusammen als ein eigenständiges Computersystem betrachtet werden können (z. B. ein PC zusammen mit einem Drucker und damit zusammenhängenden Speichervorrichtungen oder ein lokales Netzwerk). Manchmal kann auf Daten, die in einem anderen System oder in einer anderen Speichervorrichtung gespeichert sind, über das durchsuchte Computersystem rechtmäßig zugegriffen werden, indem eine Verbindung mit anderen Computersystemen hergestellt wird. Diese Situation, in der über Telekommunikationsnetzwerke Verbindungen mit anderen Computersystemen in demselben Hoheitsgebiet bestehen (wie Wide Area Network oder Internet), wird in Absatz 2 behandelt.

189. Obwohl die Durchsuchung und Beschlagnahme eines „Computerdatenträgers, auf dem Computerdaten gespeichert sein können“ (Absatz 1 Buchstabe b) aufgrund traditioneller Durchsuchungsbefugnisse erfolgen kann, erfordert die Durchführung einer Computerdurchsuchung oft die Durchsuchung sowohl des Computersystems als auch aller damit zusammenhängenden Speichermedien für Computerdaten (z. B. Disketten), die sich in der unmittelbaren Umgebung des Computersystems befinden. Aufgrund dieser Verbindung beinhaltet

Absatz 1 eine umfassende, beide Situationen abdeckende gesetzliche Befugnis.

190. Artikel 19 findet auf gespeicherte Computerdaten Anwendung. Hier stellt sich die Frage, ob eine ungeöffnete E-Mail, die sich in der Mailbox eines ISP befindet, bis der Empfänger sie auf sein Computersystem herunterlädt, als gespeicherte Computerdaten oder als Daten im Übertragungsprozess anzusehen sind. Nach dem Recht einiger Vertragsparteien ist diese E-Mail-Nachricht Teil einer Kommunikation und auf ihren Inhalt kann nur mit einer Erhebungsbefugnis zugegriffen werden, während in anderen Rechtsordnungen eine solche Nachricht als gespeicherte Daten angesehen wird, auf die Artikel 19 Anwendung findet. Die Vertragsparteien sollen daher ihre Rechtsvorschriften im Hinblick auf diesen Punkt überprüfen, um die für ihr innerstaatliches Rechtssystem geeignete Maßnahme zu bestimmen.

191. Verwendet wird der Ausdruck „durchsuchen oder in ähnlicher Weise darauf Zugriff nehmen“. Durch den Gebrauch des traditionellen Wortes „durchsuchen“ soll zum Ausdruck gebracht werden, dass der Staat die Befugnis zur Durchführung einer Zwangsmaßnahme ausübt und dass die Befugnis, von der hier die Rede ist, der traditionellen Durchsuchung entspricht. Der Begriff „durchsuchen“ bedeutet Daten suchen, lesen, einsehen oder überprüfen. Er beinhaltet sowohl die Suche nach als auch die Durchsuchung (Prüfung) von Daten. Auf der anderen Seite hat das Wort „Zugriff“ eine neutrale Bedeutung, entspricht jedoch genauer der modernen Computerterminologie. Die beiden Ausdrücke werden benutzt, um die traditionellen Begriffe mit der modernen Terminologie zu verbinden.

192. „In ihrem Hoheitsgebiet“ heißt es deshalb, weil daran erinnert werden soll, dass diese Bestimmung, wie alle in diesem Abschnitt enthaltenen Artikel, nur Maßnahmen betrifft, die auf nationaler Ebene zu treffen sind.

193. Nach Absatz 2 wird den Ermittlungsbehörden ermöglicht, ihre Durchsuchung oder ähnlichen Zugriff auf ein anderes Computersystem oder einen Teil davon auszuweiten, wenn sie Grund zu der Annahme haben, dass die gesuchten Daten in diesem anderen Computersystem gespeichert sind. Dieses andere Computersystem oder der Teil davon muss sich jedoch auch „in ihrem Hoheitsgebiet“ befinden.

194. Das Übereinkommen schreibt nicht vor, wie eine Ausweitung einer Durchsuchung genehmigt oder durchgeführt werden soll. Dies bleibt dem innerstaatlichen Recht überlassen. Es folgen einige Beispiele für mögliche Bedingungen: Eine Justizbehörde oder eine andere Behörde, welche die Durchsuchung eines bestimmten Computersystems genehmigt hat , wird ermächtigt, auch die Ausweitung der Durchsuchung oder des ähnlichen Zugriffs auf ein verbundenes System zu genehmigen, wenn sie Grund zu der Annahme hat (in dem nach dem innerstaatlichen Recht und Menschenrechtsgarantien erforderlichen Maß), dass die speziellen Daten, die gesucht werden, in dem verbundenen Computersystem enthalten sein könnten. Oder es werden die Ermittlungsbehörden dazu ermächtigt, eine genehmigte Durchsuchung oder ähnlichen Zugriff auf ein bestimmtes Computersystem auf ein damit verbundenes Computersystem auszuweiten, wenn es ähnliche Gründe zu der Annahme gibt, dass die speziellen Daten, die gesucht werden, in dem anderen Computersystem gespeichert sind. Man könnte auch die Befugnisse zur Durchsuchung oder zum Zugriff in ähnlicher Weise koordiniert und zügig an beiden Orten ausüben. In allen Fällen müssen die zu durchsuchenden Daten rechtmäßig von dem ursprünglichen System aus zugänglich oder für dieses verfügbar sein.

195. In diesem Artikel wird auf die „grenzüberschreitende Durchsuchung und Beschlagnahme“ nicht eingegangen, bei der Staaten im Hoheitsgebiet anderer Staaten Daten durchsuchen und beschlagnahmen können, ohne die in der Rechtshilfe üblichen Geschäftswege einzuhalten. Dieses Thema wird nachstehend im Kapitel über die internationale Zusammenarbeit behandelt.

196. In Absatz 3 geht es um die Ermächtigung der zuständigen Behörden zur Beschlagnahme oder ähnlichen Sicherstellung der aufgrund von Absatz 1 oder 2 erlangten Daten. Dazu gehört die Befugnis, Computer-Hardware und Speichermedien für Computerdaten zu beschlagnahmen. In bestimmten Fällen, z. B. wenn Daten in einzigartigen Betriebssystemen so gespeichert sind, dass sie nicht kopiert werden können, ist es unvermeidbar, den Datenträger als Ganzes zu beschlagnahmen. Dies kann auch erforderlich sein, wenn der Datenträger untersucht werden soll, damit alte Daten, die zwar überschrieben wurden, jedoch Spuren auf dem Datenträger hinterlassen haben, wiedererlangt werden können.

197. In diesem Übereinkommen bezieht sich „beschlagnahmen“ auf die Wegnahme des physischen Mediums, auf dem Daten oder Informationen aufgezeichnet sind, oder auf die Anfertigung und Einbehaltung einer Kopie dieser Daten oder Informationen. Der Begriff beinhaltet auch die Benutzung oder Beschlagnahme von Programmen, die erforderlich sind, um auf die zu beschlagnahmenden Daten zugreifen zu können. Neben dem traditionellen Begriff „beschlagnahmen“ wird auch der Ausdruck „in ähnlicher Weise sicherstellen“ benutzt, um auch andere Methoden zu erfassen, mit denen nicht greifbare Daten entfernt oder unzugänglich gemacht werden können oder mit denen die Verfügungsgewalt über diese Daten in der Computerumgebung auf andere Weise übernommen wird. Da sich diese Maßnahmen auf gespeicherte nicht greifbare Daten beziehen, müssen die zuständigen Behörden zusätzliche Maßnahmen zur Sicherung der Daten ergreifen, d. h. sie müssen „die Datenintegrität bewahren“ und dürfen die „Verwahrungskette“ nicht unterbrechen, was bedeutet, dass die kopierten oder entfernten Daten in dem Zustand erhalten werden müssen, in dem sie sich zum Zeitpunkt der Beschlagnahme befanden, und während des Strafverfahrens nicht verändert werden dürfen. Der Begriff bezieht sich auch auf die Übernahme der Verfügungsgewalt über und die Wegnahme von Daten.

198. Das Unzugänglichmachen von Daten kann beinhalten, dass die Daten verschlüsselt werden oder Personen der Zugriff auf diese Daten auf andere technische Weise verweigert wird. Diese Maßnahme wäre in Situationen nützlich, die eine Gefährdung oder das Risiko eines gesellschaftlichen Schadens beinhalten, wie z. B. bei Virusprogrammen oder Anleitungen zur Herstellung von Viren oder Bomben, oder in Fällen, in den die Daten oder deren Inhalt ungesetzlich sind, wie z. B. bei Kinderpornografie. Der Begriff „entfernen“ wird benutzt, um zum Ausdruck zu bringen, dass die Daten zwar entfernt oder unzugänglich gemacht, jedoch nicht zerstört werden und weiterhin vorhanden sind. Die Daten werden dem Ver-

dächtigen vorübergehend entzogen, können ihm jedoch nach Abschluss der strafrechtlichen Ermittlungen oder des Strafverfahrens zurückgegeben werden.

199. Die Beschlagnahme von Daten oder ihre Sicherstellung in ähnlicher Weise hat also zwei Funktionen: 1) das Sammeln von Beweisen, z. B. durch Kopieren der Daten, und 2) die Konfiszierung von Daten, z. B. durch Kopieren der Daten und anschließendem Unzugänglichmachen oder Entfernen der Originaldaten. Die Beschlagnahme beinhaltet keine endgültige Löschung der beschlagnahmten Daten.

200. Absatz 4 enthält eine Zwangsmaßnahme zur Erleichterung der Durchsuchung und Beschlagnahme von Computerdaten. Dabei geht es um das praktische Problem, dass es angesichts der Menge von Daten, die verarbeitet und gespeichert werden können, der angewandten Sicherheitsmaßnahmen und der Art des Computerbetriebs schwierig sein kann, auf die Daten, die als Beweismittel gesucht werden, Zugriff zu erhalten oder sie zu erkennen. Es wird anerkannt, dass es erforderlich sein kann, Systemverwalter, die das Computersystem besonders gut kennen, zu technischen Einzelheiten zu befragen, wie die Durchsuchung am besten vorzunehmen ist. Mit dieser Bestimmung wird daher den Strafverfolgungsbehörden gestattet, einen Systemverwalter dazu zu verpflichten, bei der Durchführung der Durchsuchung und Beschlagnahme in vernünftigem Maße behilflich zu sein.

201. Diese Befugnis dient nicht allein den Ermittlungsbehörden. Ohne eine derartige Zusammenarbeit könnten die Ermittlungsbehörden am Durchsuchungsort verbleiben und den Zugang zum Computersystem für einen langen Zeitraum sperren, während sie die Durchsuchung vornehmen. Dies könnte für rechtmäßige Unternehmen oder Kunden sowie für Nutzer von Computerdiensten, denen der Zugriff auf Daten während dieser Zeit verweigert wird, eine wirtschaftliche Belastung darstellen. Eine Maßnahme, die kenntnisreiche Personen zur Zusammenarbeit verpflichtet, würde dazu beitragen, die Suche sowohl für die Strafverfolgungsbehörden als auch für betroffene unschuldige Personen effizienter und kostengünstiger zu gestalten. Wenn ein Systemverwalter gesetzlich zur Hilfeleistung verpflichtet wird, kann er auch von einer vertraglichen oder sonstigen Verpflichtung, die ihn an der Weitergabe von Daten hindert, entbunden werden.

202. Angeordnet werden kann die Erteilung von Auskünften, die erforderlich sind, um die Durchsuchung und Beschlagnahme, oder auch den Zugriff in ähnlicher Weise oder die Sicherstellung, durchführen zu können. Die Erteilung dieser Auskünfte ist jedoch auf das „vernünftige“ Maß beschränkt. Unter bestimmten Umständen könnte es vernünftig sein, den Ermittlungsbehörden ein Passwort oder eine andere Sicherheitsmaßnahme zu offenbaren. Unter anderen Umständen könnte man dies jedoch nicht als vernünftig bezeichnen, z. B. wenn die Offenbarung eines Passworts oder einer anderen Sicherheitsmaßnahme die Privatsphäre anderer Nutzer oder andere Daten, deren Durchsuchung nicht genehmigt ist, gefährden könnte. In einem solchen Fall könnte die Erteilung der „notwendigen Auskünfte“ in der Bereitstellung der eigentlichen, von den zuständigen Behörden angeforderten Daten in verständlicher und lesbarer Form bestehen.

203. Gemäß Absatz 5 dieses Artikels unterliegen diese Maßnahmen den auf der Grundlage von Artikel 15 dieses Übereinkommens in den innerstaatlichen Rechtsvorschriften vorgesehenen Bedingungen und Garantien. Diese Bedingungen können auch Bestimmungen über den Einsatz von Zeugen und Sachverständigen und deren Entschädigung enthalten.

204. Die Verfasser erörterten ferner im Zusammenhang mit Absatz 5, ob betroffene Parteien von der Durchführung der Durchsuchung informiert werden sollen. In der „On-line-Welt“ ist vielleicht weniger offensichtlich, dass Daten durchsucht und beschlagnahmt (kopiert) worden sind, als wenn eine Beschlagnahme in der „Off-line-Welt“ stattgefunden hat, wo beschlagnahmte Gegenstände physisch fehlen. Nach den Rechtsvorschriften einiger Vertragsparteien ist es nicht erforderlich, von einer traditionellen Durchsuchung Mitteilung zu machen. Wenn es nach dem Übereinkommen erforderlich wäre, von einer Computerdurchsuchung Mitteilung zu machen, würde dies zu einem Widerspruch in den Rechtsvorschriften dieser Vertragsparteien führen. Andererseits könnten manche Vertragsparteien die Benachrichtigung als wesentlichen Bestandteil der Maßnahme ansehen, um die Unterscheidung zwischen einer Durchsuchung gespeicherter Computerdaten (die im Allgemeinen keine heimliche Maßnahme darstellen soll) und dem Abfangen fließender Daten (die eine heimliche Maßnahme ist, siehe Artikel 20 und 21) aufrechtzuerhalten. Daher ist die Frage der Benachrichtigung durch innerstaatliche Rechtsvorschriften zu klären. Wenn die Vertragsparteien eine obligatorische Benachrichtigung von Betroffenen erwägen, so sollte berücksichtigt werden, dass eine solche Benachrichtigung die Ermittlungen gefährden könnte. Wenn diese Gefahr besteht, könnte ein Aufschub der Benachrichtigung erwogen werden.

Titel 5
Erhebung von Computerdaten in Echtzeit

205. Artikel 20 und 21 sehen die Echtzeit-Erhebung von Verkehrsdaten und Inhaltsdaten vor, die mit bestimmten mittels eines Computersystems übertragenen Kommunikationen in Zusammenhang stehen. Die Bestimmungen beziehen sich auf die Echtzeit-Erhebung solcher Daten durch die zuständigen Behörden sowie deren Erhebung durch Diensteanbieter. Die Verpflichtung zur vertraulichen Behandlung ist auch Gegenstand der Bestimmungen.

206. Die Überwachung der Telekommunikation bezieht sich in der Regel auf herkömmliche Telekommunikationsnetzwerke. Diese können in Infrastrukturen von Kabeln – Drahtkabeln oder optischen Kabeln – sowie Verbindungen mit drahtlosen Netzwerken bestehen und umfassen auch Mobiltelefonsysteme und Mikrowellenübertragungssysteme. Heutzutage werden mobile Datenübertragungen auch durch ein System spezieller Satellitennetzwerke erleichtert. Computernetzwerke können auch in einem unabhängigen festen Kabelgebilde bestehen; sie werden aber häufiger durch über Telekommunikationsinfrastrukturen hergestellte Verbindungen als ein virtuelles Netzwerk betrieben und ermöglichen damit die Einrichtung globaler Computernetzwerke oder Netzwerkverknüpfungen. Der Unterschied zwischen Telekommunikation und Computerdatenübertagungen und die typischen Merkmale ihrer Infrastrukturen sind angesichts der Konvergenz von Telekommunikations- und

Informationstechnologie kaum erkennbar. Somit wird die Art und Weise, in der Einzelvorrichtungen oder eine Einheit von Vorrichtungen verbunden werden können, durch die Bestimmung des Begriffs „Computersystem“ nach Artikel 1 nicht eingeschränkt. Artikel 20 und 21 finden demnach auf bestimmte mittels eines Computersystems übertragene Kommunikationen, die die Übertragung der Kommunikation über Telekommunikationsnetzwerke vor deren Empfang durch ein anderes Computersystem einschließen können, Anwendung.

207. Artikel 20 und 21 unterscheiden nicht zwischen Telekommunikationen und Computersystemen in öffentlichem oder privatem Eigentum oder zwischen der Nutzung von Systemen und Datenübertragungsdiensten, die der Öffentlichkeit oder bestimmten Benutzergruppen oder Privatparteien angeboten werden. Die Bestimmung des Begriffs „Diensteanbieter“ in Artikel 1 bezieht sich auf öffentliche und private Einrichtungen, die es Nutzern ihrer Dienste ermöglichen, mittels eines Computersystems zu kommunizieren.

208. Dieser Titel regelt die Erhebung von Beweisdaten, die in aktuell erzeugten Kommunikationen enthalten sind und im Zeitpunkt der Kommunikation erhoben werden (d. h. „Echtzeit“). Die Daten sind von ihrer Form her immateriell (z. B. in Form von Stimmenübertragungen oder Übertragungen elektronischer Impulse). Der Datenfluss wird durch die Erhebung nicht nennenswert gestört und die Kommunikation erreicht den gewünschten Empfänger. Anstelle einer physischen Beschlagnahme der Daten wird eine Aufzeichnung (d. h. eine Kopie) der übermittelten Daten erstellt. Die Erhebung dieser Beweisdaten findet innerhalb einer bestimmten Zeit statt. Eine Genehmigung zur Erhebung wird in Bezug auf ein künftiges Ereignis (d. h. eine künftige Datenübertragung) eingeholt.

209. Bei den Daten, die erfasst werden können, wird zwischen zwei Arten unterschieden, und zwar zwischen Verkehrsdaten und Inhaltsdaten. „Verkehrsdaten“ bedeutet nach der Begriffsbestimmung in Artikel 1 Buchstabe d Computerdaten in Zusammenhang mit einer Kommunikation unter Nutzung eines Computersystems, die von einem Computersystem, das Teil der Kommunikationskette war, erzeugt wurden und aus denen Ursprung, Ziel, Leitweg, Uhrzeit, Datum, Umfang und Dauer der Kommunikation oder die Art des Trägerdienstes hervorgehen. Der Begriff „Inhaltsdaten“ wird in dem Übereinkommen nicht definiert; er bezieht sich aber auf den Kommunikationsinhalt, d. h. die Bedeutung oder den Tenor der Kommunikation, oder die Nachricht oder Information, die durch die Kommunikation übermittelt wird (im Gegensatz zu Verkehrsdaten).

210. In vielen Staaten wird zwischen der Echtzeit-Erhebung von Inhaltsdaten und der Echtzeit-Erhebung von Verkehrsdaten sowohl im Hinblick auf die rechtlichen Voraussetzungen, die zur Genehmigung einer derartigen Untersuchungsmaßnahme erforderlich sind, als auch in Bezug auf die Straftaten, derentwegen diese Maßnahme angewandt werden kann, unterschieden. Es wird zwar anerkannt, dass mit beiden Datenarten Belange der Privatsphäre verbunden sein können, jedoch sind viele Staaten der Auffassung, dass Belange der Privatsphäre bei Inhaltsdaten wegen der Art des Kommunikationsinhalts oder der Nachricht eine größere Rolle spielen. In Bezug auf die Echtzeit-Erhebung von Inhaltsdaten können im Vergleich zu Verkehrsdaten größere Beschränkungen auferlegt werden. Um dieser Unterscheidung im Sinne dieser Staaten gerecht zu werden, wird in den Überschriften der Artikel des Übereinkommens, das zwar für die Praxis anerkennt, dass Daten in beiden Situationen erhoben und aufgezeichnet werden, normativ die Erhebung von Verbindungsdaten als „Echtzeit-Erhebung“ und die Erhebung von Inhaltsdaten als „Echtzeit-Abfangen“ bezeichnet *[Anm. d. Übers.: Diese sprachliche Unterscheidung findet sich nur in der englischen und französischen Sprachfassung]*.

211. In einigen Staaten unterscheidet das geltende Recht nicht zwischen der Erhebung von Verkehrsdaten und der Erhebung von Inhaltsdaten, weil im Gesetz nicht im Hinblick auf Unterschiede bei den Belangen der Privatsphäre unterschieden wird oder die technischen Erhebungsverfahren bei beiden Maßnahmen sehr ähnlich sind. Somit sind die rechtlichen Voraussetzungen für die Genehmigung der Durchführung der Maßnahmen und die Straftaten, derentwegen die Maßnahmen angewandt werden können, die gleichen. Das Übereinkommen trägt diesem Umstand auch durch die gemeinsame Verwendung des Begriffs „erheben oder aufzeichnen“ im Wortlaut der Artikel 20 und 21 Rechnung.

212. Im Hinblick auf die Echtzeit-Erhebung von Inhaltsdaten schreibt das Gesetz oftmals vor, dass diese Maßnahme nur im Rahmen der Ermittlung schwerer Straftaten oder von Kategorien schwerer Straftaten zulässig ist. Diese Straftaten erscheinen zu diesem Zweck im innerstaatlichen Recht häufig dadurch als schwere Straftaten, dass sie in einer Liste der anwendbaren Straftaten aufgeführt sind oder durch einen Verweis auf eine bestimmte Höchststrafe, die wegen dieser Straftat verhängt werden kann, unter diese Kategorie fallen. Daher bestimmt Artikel 21 im Zusammenhang mit der Erhebung von Inhaltsdaten eindeutig, dass die Vertragsparteien nur verpflichtet sind, die Maßnahme „in Bezug auf eine Reihe schwerer Straftaten, die durch ihr innerstaatliches Recht zu bestimmen sind“ zu treffen.

213. Artikel 20, der die Erhebung von Verkehrsdaten betrifft, ist dagegen weniger restriktiv und bezieht sich grundsätzlich auf jede vom Übereinkommen erfasste Straftat. Artikel 14 Absatz 3 bestimmt jedoch, dass eine Vertragspartei sich das Recht vorbehalten kann, die Maßnahme nur auf die in dem Vorbehalt angegebenen Straftaten oder Arten von Straftaten anzuwenden, wobei die Reihe dieser Straftaten oder Arten von Straftaten nicht enger gefasst sein darf als diejenige, auf die sie die Maßnahme der Erhebung von Inhaltsdaten anwendet. Jedoch soll eine Vertragspartei, die einen solchen Vorbehalt macht, diesen beschränken, um die Anwendung der Maßnahme der Erhebung von Verkehrsdaten weitgehendst zu ermöglichen.

214. Einige Staaten würden die in dem Übereinkommen festgelegten Straftaten normalerweise nicht als hinreichend schwer ansehen, um die Erhebung von Inhaltsdaten oder in manchen Fällen sogar die Erfassung von Verkehrsdaten zu gestalten. Dennoch sind solche Verfahren für die Ermittlung einiger der nach dem Übereinkommen festgelegten Straftaten wie etwa Handlungen, die rechtswidrigen Zugriff auf Computersysteme sowie das Verbreiten von Viren und Kinderpornografie betreffen, oft unerlässlich. Die Störungsquelle kann z. B. in manchen Fällen nicht ohne Echtzeit-Erhebung von Verkehrsdaten

ermittelt werden. Bisweilen ist es nicht möglich, die Art der Kommunikation ohne Echtzeit-Erhebung von Inhaltsdaten zu erkennen. Derartige Straftaten implizieren aufgrund ihrer Art und des Übertragungswegs den Einsatz von Computertechnologien. Daher sollte die Anwendung technischer Mittel für die Ermittlung dieser Straftaten zulässig sein. Angesichts der Empfindlichkeiten bei dem Thema Erhebung von Inhaltsdaten überlässt das Übereinkommen den Anwendungsbereich dieser Maßnahme jedoch der Bestimmung durch das innerstaatliche Recht. Da einige Länder die Erhebung von Verkehrsdaten der Erhebung von Inhaltsdaten rechtlich gleichstellen, ist eine Vorbehaltsmöglichkeit im Hinblick auf die Einschränkung der Anwendbarkeit der erstgenannten Maßnahme zulässig, jedoch nur in dem Umfang, in dem eine Vertragspartei die Maßnahme der Echtzeit-Erhebung von Inhaltsdaten einschränkt. Die Vertragsparteien sollten dennoch eine Anwendung der beiden Maßnahmen auf die in Kapitel II Abschnitt 1 des Übereinkommens festgelegten Straftaten erwägen, damit ein wirksames Verfahren für die Ermittlung dieser Computerstraftaten geschaffen wird.

215. Die Bedingungen und Garantien im Hinblick auf die Befugnisse und Verfahren, die sich auf die Echtzeit-Erhebung von Inhaltsdaten und die Echtzeit-Erhebung von Verkehrsdaten beziehen, unterliegen den Artikeln 14 und 15. Da die Erhebung von Inhaltsdaten einen erheblichen Eingriff in das Privatleben darstellt, bedarf es zwingender Garantien, um ein angemessenes Gleichgewicht zwischen den Belangen der Justiz und den Grundrechten des Einzelnen herzustellen. Im Bereich der Erhebung von Inhaltsdaten sieht dieses Übereinkommen außer der Beschränkung der Befugnis der Erhebung von Inhaltsdaten auf Ermittlungen wegen Handlungen, die nach innerstaatlichem Recht schwere Straftaten darstellen, keine bestimmten Garantien vor. Gleichwohl greifen nach innerstaatlichen Rechtsnormen die folgenden einschlägigen wichtigen Bedingungen und Garantien, und zwar die Kontrolle durch ein Gericht oder eine unabhängige Instanz, die genaue Bestimmung der abzufangenden Daten oder Personen, die Erforderlichkeit, Subsidiarität und Angemessenheit (z. B. Vortaten, die zum Ergreifen der Maßnahme berechtigen, die Unwirksamkeit anderer weniger eingreifender Maßnahmen), die Beschränkung der Dauer des Abfangens, das Beschwerderecht. Viele dieser Garantien erinnern an die Europäische Menschenrechtskonvention und das daran anknüpfende Fallrecht (siehe Entscheidungen in Sachen Klass[5]), Kruslin[6]), Huvig[7]), Malone[8]), Halford[9]) und Lambert[10])). Einige dieser Garantien finden auch bei der Erhebung von Verkehrsaten in Echtzeit Anwendung.

Erhebung von Verkehrsdaten in Echtzeit (Artikel 20)

216. Frühere Verkehrsdaten können oftmals nicht mehr verfügbar oder wertlos sein, weil der Eindringling den Leitweg geändert hat. Aus diesem Grunde stellt die Echtzeit-Erhebung von Verkehrsdaten eine wesentliche Ermittlungsmaßnahme dar. Artikel 20 behandelt die Echtzeit-Erhebung und Aufzeichnung von Verkehrsdaten zum Zwecke spezifischer strafrechlicher Ermittlungen oder Verfahren.

217. Die Erhebung von Verkehrsdaten im Zusammenhang mit Telekommunikation (z. B. Telefongespräche) stellt von jeher ein nützliches Ermittlungsinstrument dar, um die Quelle oder den Empfänger (z. B. Telefonnummern) und die damit zusammenhängenden Daten (z. B. Zeit, Datum und Dauer) verschiedener Arten rechtswidriger Kommunikation (z. B. strafbare Drohung und Belästigung, strafbare Verabredung, betrügerische falsche Darstellung von Tatsachen) sowie von Kommunikationen, die Beweise für vergangene oder künftige Straftaten (z. B. Drogenhandel, Mord, Wirtschaftsstraftaten usw.) liefern, zu ermitteln.

218. Computerkommunikationen können für dieselbe Art von Kriminalität Beweise darstellen oder liefern. Da über die Computertechnologie jedoch große Datenmengen mit Texten, visuellen Darstellungen und Tönen übertragen werden können, birgt sie auch ein höheres Potenzial für die Begehung von Straftaten, die das Verbreiten rechtswidriger Inhalte (z. B. Kinderpornografie) betreffen. Da Computer große Datenmengen, die oft privater Natur sind, speichern können, kann potenziell ebenso erheblicher Schaden – sei es auf ökonomischer, gesellschaftlicher oder persönlicher Ebene – angerichtet werden, wenn die Integrität der Daten beeinträchtigt wird. Da die Computertechnologie auf der Datenverarbeitung beruht, und zwar sowohl als Endprodukt als auch als Teil der Betriebsfunktion (z. B. die Ausführung von Computerprogrammen), kann eine Störung dieser Daten verheerende Auswirkungen auf den ordnungsgemäßen Betrieb von Computersystemen haben. Wird ein rechtswidriges Verbreiten von Kinderpornografie, ein rechtswidriger Zugriff auf ein Computersystem oder ein Eingriff in die Funktionsweise des Computersystems oder die Integrität von Daten insbesondere aus der Entfernung wie aus dem Internet vorgenommen, ist es erforderlich und unabdingbar, den Weg der Kommunikationen vom Opfer zum Täter zurückzuverfolgen. Daher kommt der Fähigkeit, Verkehrsdaten im Zusammenhang mit Computerkommunikationen zu erheben, die gleiche – wenn nicht sogar größere – Bedeutung zu wie im Rahmen der rein herkömmlichen Telekommunikation. Diese Ermittlungsmethode kann die Uhrzeit, das Datum, die Quelle und den Empfänger der Kommunikationen des Verdächtigen in Beziehung zu der Uhrzeit des Eindringens in das System des Opfers setzen, weitere Opfer feststellen oder Verbindung zu Komplizen aufzeigen.

219. Nach diesem Artikel müssen die betreffenden Verkehrsdaten mit bestimmten Kommunikationen im Hoheitsgebiet der Vertragspartei in Zusammenhang stehen. Von den bestimmten „Kommunikationen“ ist im Plural die Rede, weil möglicherweise Verkehrsdaten im Zusammenhang mit mehreren Kommunikationen zu erheben sind, um die Benutzerquelle oder den Empfänger zu ermitteln (z. B. kann es in einem Haushalt, in dem verschiedene Personen dieselben Telekommunikationseinrichtungen benutzen, notwendig sein, verschiedene Kommunikationen mit der Gelegenheit einzelner Personen zur Benutzung des Computersystems in Beziehung zu setzen). Zu Kommunikationen, deren Verkehrsdaten erhoben oder aufgezeichnet werden können, sind jedoch genaue Angaben zu machen. Das Übereinkommen verlangt oder erlaubt also keine willkürliche Überwachung und Erhebung von großen Verkehrsdatenmengen. Es erlaubt keine „Fischzüge“, bei denen man hofft, kriminelle Aktivitäten zu entdecken, im Gegensatz zu Ermittlungen wegen bestimmter krimineller Handlungen. In dem gerichtlichen oder sonstigen Beschluss, mit dem die

Erhebung genehmigt wird, sind die Kommunikationen anzugeben, auf die sich die Erhebung der Verkehrsdaten bezieht.

220. Vorbehaltlich des Absatzes 2 sind die Vertragsparteien nach Absatz 1 Buchstabe a verpflichtet, ihren zuständigen Behörden die Befugnis zu erteilen, Verkehrsdaten durch Anwendung technischer Mittel zu erheben oder aufzuzeichnen. Dieser Artikel enthält keine Angaben dazu, wie die Erhebung technisch durchzuführen ist, und es werden keine Verpflichtungen in technischer Hinsicht genannt.

221. Nach Absatz 1 Buchstabe b sind die Vertragsparteien darüber hinaus verpflichtet, sicherzustellen, dass ihre zuständigen Behörden befugt sind, einen Diensteanbieter zu zwingen, Verkehrsdaten zu erheben oder aufzuzeichnen oder bei der Erhebung oder Aufzeichnung solcher Daten mit den zuständigen Behörden zusammenzuarbeiten und sie zu unterstützen. Diese Verpflichtung in Bezug auf den Diensteanbietern gilt nur insoweit, als die Erhebung oder Aufzeichnung oder die Zusammenarbeit und Unterstützung im Rahmen des dem Diensteanbieter zur Verfügung stehenden technischen Standards erfolgen kann. Der Artikel verpflichtet Diensteanbieter nicht, für einen technischen Standard Sorge zu tragen, der ihnen die Erhebung, Aufzeichnung, Zusammenarbeit oder Unterstützung ermöglicht. Es wird von ihnen nicht verlangt, dass sie neue Geräte anschaffen oder entwickeln, Experten hinzuziehen oder in eine kostspielige Rekonfiguration ihrer Systeme investieren. Wenn ihre Systeme und ihr Personal jedoch den technischen Standard aufweisen, um solch eine Erhebung und Aufzeichnung vorzunehmen und eine derartige Zusammenarbeit oder Unterstützung zu leisten, sind sie nach diesem Artikel verpflichtet, die dazu notwendigen Maßnahmen zu ergreifen. Das System kann zum Beispiel in der erforderlichen Weise konfiguriert sein oder dem Diensteanbieter können bereits Computerprogramme vorliegen, die zwar die Durchführung solcher Maßnahmen ermöglichen würden, aber im Rahmen des üblichen Betriebs des Diensteanbieters gewöhnlich nicht ausgeführt oder benutzt werden. Der Diensteanbieter ist nach diesem Artikel verpflichtet, diese Eigenschaften wie gesetzlich vorgeschrieben einzusetzen oder in Gang zu setzen.

222. Da diese Maßnahme auf nationaler Ebene durchzuführen ist, beziehen die Maßnahmen sich auf die Erhebung oder Aufzeichnung bestimmter Kommunikationen im Hoheitsgebiet der Vertragspartei. Daraus ergibt sich in der Praxis, dass die Verpflichtungen in der Regel dann gelten, wenn der Diensteanbieter in diesem Hoheitsgebiet über eine physische Infrastruktur oder Geräte verfügt, mit denen die Maßnahmen durchgeführt werden können, auch wenn er dort nicht seiner Haupttätigkeit nachgeht oder seinen Hauptsitz hat. Im Sinne dieses Übereinkommens gilt eine Kommunikation als im Hoheitsgebiet einer Vertragspartei vorgenommen, wenn sich einer der Kommunikationspartner (Benutzer oder Computer) in dem betreffenden Hoheitsgebiet befindet oder wenn sich der Computer oder das Telekommunikationsgerät, worüber die Kommunikation erfolgt, in dem Hoheitsgebiet befindet.

223. Im Allgemeinen stellen die beiden in Absatz 1 Buchstaben a und b genannten Möglichkeiten zur Erhebung von Verkehrsdaten keine Alternativen dar. Vorbehaltlich des Absatzes 2 muss eine Vertragspartei dafür Sorge tragen, dass beide Maßnahmen durchgeführt werden können. Diese Notwendigkeit besteht, weil die Strafverfolgungsbehörden einer Vertragspartei die Möglichkeit haben müssen, die Erhebung oder Aufzeichnung von Verkehrsdaten selbst vorzunehmen (Absatz 1 Buchstabe a), wenn ein Diensteanbieter technisch nicht in der Lage ist, dieser Aufgabe nachzukommen (Absatz 1 Buchstabe b). Ebenso ist eine Verpflichtung zur Zusammenarbeit mit den zuständigen Behörden und deren Unterstützung bei der Erhebung oder Aufzeichnung von Verkehrsdaten nach Absatz 1 Buchstabe b Ziffer ii unsinnig, wenn die zuständigen Stellen nicht befugt sind, die Verkehrsdaten selbst zu erheben oder aufzuzeichnen. Ferner dürften die Ermittlungsbehörden bei einigen lokalen Netzwerken, an denen möglicherweise kein Diensteanbieter beteiligt ist, nur die Möglichkeit haben, die Erfassung oder Aufzeichnung selbst vorzunehmen. Die beiden in Absatz 1 Buchstaben a und b genannten Maßnahmen müssen nicht in allen Fällen angewandt werden; der Artikel schreibt jedoch die Verfügbarkeit beider Methoden vor.

224. Diese zweifache Verpflichtung bereitet jedoch manchen Staaten, in denen die Strafverfolgungsbehörden Daten in Telekommunikationssystemen nur mit Unterstützung eines Diensteanbieters oder nicht heimlich ohne dessen Wissen abfangen konnten, Schwierigkeiten. Daher findet dieser Umstand in Absatz 2 Berücksichtigung. Kann eine Vertragspartei die in Absatz 1 Buchstabe a bezeichneten Maßnahmen angesichts „der bestehenden Grundsätze ihrer innerstaatlichen Rechtsordnung“ nicht ergreifen, so kann sie stattdessen in anderer Weise vorgehen und etwa die Diensteanbieter lediglich verpflichten, die technische Ausrüstung bereitzustellen, die erforderlich ist, um die Echtzeit-Erhebung von Verkehrsdaten durch die Strafverfolgungsbehörden sicherzustellen. In diesem Fall greifen nach wie vor alle anderen Einschränkungen in Bezug auf Hoheitsgebiet, Bestimmtheit der Kommunikation und Anwendung technischer Mittel.

225. Die Echtzeit-Erhebung von Verkehrsdaten ist wie die Echtzeit-Erhebung von Inhaltsdaten nur wirksam, wenn die Personen, gegen die ermittelt wird, davon keine Kenntnis haben. Die Erhebung erfolgt heimlich und ist so durchzuführen, dass die Kommunikationspartner diese Maßnahme nicht bemerken. Diensteanbieter und ihre Mitarbeiter, die über die Erhebung unterrichtet sind, müssen daher zur Geheimhaltung verpflichtet werden, damit das Verfahren erfolgreich durchgeführt werden kann.

226. Absatz 3 verpflichtet die Vertragsparteien, die erforderlichen gesetzgeberischen und anderen Maßnahmen zu treffen, um einen Diensteanbieter zu verpflichten, die tatsächliche Ausführung einer der in diesem Artikel im Zusammenhang mit der Echtzeit-Erhebung von Verkehrsdaten aufgeführten Maßnahmen sowie Auskünfte darüber vertraulich zu behandeln. Diese Bestimmung gewährleistet nicht nur die Vertraulichkeit der Ermittlung, sondern befreit den Diensteanbieter auch von jeglicher vertraglicher oder sonstiger rechtlicher Verpflichtung, Kunden darüber zu unterrichten, dass Daten über sie erfasst werden. Absatz 3 kann durch die Schaffung gesetzlich verankerter eindeutiger Verpflichtungen umgesetzt werden. Andererseits können die Vertragsparteien die Vertraulichkeit der Maßnahme auch aufgrund anderer innerstaatlicher Rechtsvorschriften sicherstellen, wie z. B. mit der Befugnis, Personen, die Straftätern

behilflich sind, indem sie sie über die Maßnahme unterrichten, wegen Behinderung der Justiz zu verfolgen. Obwohl die spezielle Voraussetzung der Vertraulichkeit (mit einer wirksamen Sanktion bei Verletzung) das bevorzugte Verfahren darstellt, kann der Rückgriff auf Straftaten der Justizbehinderung eine Alternative zur Verhinderung der unerlaubten Weitergabe darstellen und genügt daher auch, um diese Bestimmung umzusetzen. Sofern ausdrückliche Verpflichtungen zur Geheimhaltung vorgesehen werden, unterliegen diese den Bedingungen und Garantien nach Artikel 14 und 15. Diese Garantien und Bedingungen sollten wegen der Vertraulichkeit der Ermittlungsmaßnahme einen angemessenen Zeitraum für die Dauer der Verpflichtung vorschreiben.

227. Wie bereits erwähnt, wiegt das Recht auf Achtung der Privatsphäre im Zusammenhang mit der Erhebung von Verkehrsdaten in der Regel weniger schwer als bei der Erhebung von Inhaltsdaten. Verkehrsdaten über die Uhrzeit, die Dauer und den Umfang der Kommunikation geben über eine Person oder ihr Denken wenige persönliche Informationen preis. Ein strengeres Gebot in Bezug auf den Schutz der Privatsphäre dürfte im Zusammenhang mit Daten über die Quelle oder den Empfänger einer Kommunikation (z. B. die aufgerufenen Websites) bestehen. Die Erhebung dieser Daten kann in manchen Fällen die Erstellung eines Profils der Interessen, der Kollegen und des sozialen Umfelds des Betroffenen ermöglichen. Demgemäß sollten die Vertragsparteien diese Gesichtspunkte berücksichtigen, wenn sie die geeigneten Garantien und rechtlichen Voraussetzungen für die Durchführung dieser Maßnahmen nach Artikel 14 und 15 festlegen.

Erhebung von Inhaltsdaten in Echtzeit (Artikel 21)

228. Die Erhebung von Inhaltsdaten im Zusammenhang mit der Telekommunikation (z. B. Telefongespräche) stellt von jeher ein sinnvolles Ermittlungsinstrument dar, um festzustellen, ob eine Kommunikation rechtswidrig ist (ob z. B. eine strafbare Drohung oder Belästigung, eine strafbare Verabredung oder betrügerische falsche Darstellung von Tatsachen Gegenstand der Kommunikation ist), und um Beweise für vergangene oder künftige Straftaten (z. B. Drogenhandel, Mord, Wirtschaftsstraftaten usw.) zu liefern. Computerkommunikationen können für dieselbe Art von Kriminalität Beweise darstellen oder erbringen. Da über die Computertechnologie jedoch große Datenmengen mit Texten, visuellen Darstellungen und Tönen übertragen werden können, birgt sie ein größeres Potenzial für die Begehung von Straftaten, die auch das Verbreiten rechtswidriger Inhalte (z. B. von Kinderpornografie) betreffen. Viele Computerstraftaten bestehen teilweise in der Übertragung von Daten wie z. B. solchen, die versandt werden, um auf ein Computersystem rechtswidrig Zugriff zu nehmen, oder in dem Verbreiten von Computerviren. Ohne das Abfangen des Inhalts der Nachricht kann die schädliche rechtswidrige Natur dieser Kommunikationen nicht in Echtzeit bestimmt werden. Ohne die Fähigkeit, im Gange befindliche Kriminalität festzustellen und zu verhüten, müssten die Strafverfolgungsbehörden sich darauf beschränken, vergangene vollendete Straftaten, die bereits Schaden angerichtet haben, zu ermitteln. Daher ist die Erhebung von Inhaltsdaten von Computerkommunikationen in Echtzeit ebenso wichtig wie die Erhebung von Telekommunikation in Echtzeit – wenn nicht sogar wichtiger.

229. „Inhaltsdaten“ beziehen sich auf den Kommunikationsinhalt der Kommunikation, d. h. die Bedeutung oder den Sinn der Kommunikation bzw. die durch die Kommunikation übermittelte Nachricht oder Information. Sie sind alles, was als Bestandteil der Kommunikation übermittelt wird und keine Verkehrsdaten darstellt.

230. Dieser Artikel stimmt mit Artikel 20 überwiegend überein. Daher finden die vorstehenden Erläuterungen zur Erhebung oder Aufzeichnung von Verkehrsdaten, zur Verpflichtung zur Zusammenarbeit und Unterstützung und zur Vertraulichkeit auch auf das Abfangen von Inhaltsdaten Anwendung. Da das Recht auf Achtung der Privatsphäre in höherem Maße Inhaltsdaten betrifft, ist die Ermittlungsmaßname auf „eine Reihe schwerer Straftaten, die durch innerstaatliches Recht zu bestimmen sind“, beschränkt.

231. Wie in den vorstehenden Erläuterungen zu Artikel 20 dargelegt, können die Bedingungen und Garantien im Hinblick auf die Echtzeit-Erhebung von Inhaltsdaten strenger sein als diejenigen, die für die Echtzeit-Erhebung von Verkehrsdaten oder die Durchsuchung und Beschlagnahme gespeicherter Daten oder einen ähnlichen Zugriff auf solche Daten oder deren Sicherung gelten.

Abschnitt 3 – Gerichtsbarkeit

Gerichtsbarkeit (Artikel 22)

232. Dieser Artikel legt eine Reihe von Kriterien fest, aufgrund deren Vertragsparteien verpflichtet sind, die Gerichtsbarkeit über die in den Artikeln 2 bis 11 des Übereinkommens aufgeführten Straftaten zu begründen.

233. Absatz 1 Buchstabe a gründet auf dem Territorialitätsprinzip. Jede Partei ist verpflichtet, die Begehung von nach dem Übereinkommen festgelegten Straftaten, die in ihrem Hoheitsgebiet begangen werden, zu bestrafen. Z. B. würde eine Partei sich territorial für zuständig erklären, wenn sowohl die Person, die ein Computersystem angreift, als auch der Geschädigte sich in ihrem Hoheitsgebiet befinden und wenn sich das angegriffene Computersystem in ihrem Hoheitsgebiet befindet, auch wenn der Angreifer sich nicht dort aufhält.

234. Es wurde erwogen, eine Bestimmung aufzunehmen, die jede Vertragspartei verpflichtet, eine Gerichtsbarkeit für Straftaten zu begründen, die auf ihren Namen eingetragene Satelliten betreffen. Die Verfasser hielten solch eine Bestimmung für überflüssig, weil rechtswidrige Datenübertragungen mit Satelliten zwangsläufig von der Erde ausgehen und/oder dort empfangen werden. Insoweit gilt ein Gerichtstand, wie er in Absatz 1 Buchstaben a bis c dargelegt ist, als bei einer Vertragspartei begründet, wenn die Übertragung von einem der dort genannten Orte ausgeht oder dort beendet wird. Soweit die mit einer Satellitenübertragung zusammenhängende Straftat von einem Staatsangehörigen einer Vertragspartei außerhalb der territorialen Gerichtsbarkeit irgendeines Staates begangen wird, wird die Zuständigkeit dieser Vertragspartei aufgrund von Absatz 1 Buchstabe d darüber hinaus begründet. Schließlich haben die Verfasser sich die Frage gestellt, ob eine Strafgerichtsbarkeit durch eine Eintragung territorial angemessen begründet werden kann, weil in vielen Fällen kein sinnvoller Zusammenhang zwischen der begangenen Straftat und dem Staat der Registrierung hergestellt werden könne, da ein Satellit lediglich als Übertragungsmittel fungiert.

235. Absatz 1 Buchstaben b und c geht von einer Variante des Territorialitätsprinzips aus. Danach ist jede Vertragspartei verpflichtet, ihre Strafgerichtsbarkeit für Straftaten zu begründen, die an Bord eines Schiffes oder Flugzeugs begangen werden, das nach ihren Rechtsvorschriften eingetragen ist. Im Allgemeinen wird diese Verpflichtung nach dem Recht vieler Staaten bereits erfüllt, weil diese Schiffe und Flugzeuge oft als erweitertes Hoheitsgebiet dieses Staates angesehen werden. Diese Art Gerichtsbarkeit ist äußerst sinnvoll, wenn das Schiff oder Flugzeug sich zur Tatzeit nicht in seinem Hoheitsgebiet befindet; demnach könnte eine Zuständigkeit nicht aufgrund von Absatz 1 Buchstabe a begründet werden. Wird die Straftat an Bord eines Schiffes oder Flugzeugs begangen, das sich außerhalb des Hoheitsgebiets der flaggeführenden Vertragspartei befindet, könnte möglicherweise kein anderer Staat die Gerichtsbarkeit ausüben, wenn diese Voraussetzung nicht bestehen würde. Wenn eine Straftat darüber hinaus an Bord eines Schiffes oder Flugzeugs begangen wird, das nur die Gewässer oder den Luftraum eines anderen Staates durchquert, kann Letzterer auf erhebliche praktische Hindernisse stoßen, die der Ausübung der Gerichtsbarkeit entgegenstehen; insoweit ist es sinnvoll, wenn der Staat, bei dem das Schiff oder Flugzeug geführt wird, auch zuständig ist.

236. Absatz 1 Buchstabe d gründet auf dem Grundsatz der Staatsangehörigkeit. Die Staatsangehörigkeitstheorie wird in der Regel von den Staaten angewandt, die in der Tradition des römischen Rechts stehen. Es bestimmt, dass die Angehörigen eines Staates auch außerhalb ihres Hoheitsgebiets zur Einhaltung des innerstaatlichen Rechts verpflichtet sind. Wenn ein Staatsangehöriger im Ausland straffällig wird, ist die Vertragspartei nach Buchstabe d verpflichtet, zur Verfolgung der Straftat fähig zu sein, sofern die Tat auch nach dem Recht des Staates, in dem sie begangen wurde, einen Straftatbestand erfüllt oder die Handlung außerhalb der territorialen Gerichtsbarkeit irgendeines Staates begangen wurde.

237. Nach Artikel 2 können die Parteien einen Vorbehalt zu den in Absatz 1 Buchstaben b, c und d enthaltenen Vorschriften in Bezug auf die Gerichtsbarkeit einlegen. Im Hinblick auf die Begründung der territorialen Gerichtsbarkeit nach Buchstabe a oder die Verpflichtung nach Absatz 3, die Gerichtsbarkeit in Fällen zu begründen, die unter den Grundsatz des „aut dedere aut judicare“ (ausliefern oder strafrechtlich verfolgen) fallen, wenn die betreffende Vertragspartei die Auslieferung des mutmaßlichen Täters wegen seiner Staatsangehörigkeit ablehnt und dieser sich in ihrem Hoheitsgebiet aufhält, ist jedoch kein Vorbehalt zulässig. Der aufgrund von Absatz 3 zu begründenden Gerichtsbarkeit bedarf es, um sicherzustellen, dass Vertragsparteien, die die Auslieferung eines eigenen Staatsangehörigen ablehnen, rechtlich in der Lage sind, ersatzweise innerstaatlich Ermittlungen und Verfahren zu betreiben, wenn die Vertragspartei, die nach den Voraussetzungen des Artikels 24 Absatz 6 dieses Übereinkommens („Auslieferung“) die Auslieferung begehrt hat, darum ersucht.

238. Die in Absatz 1 aufgeführten Grundlagen für die Gerichtsbarkeit sind nicht ausschließlich. Nach Absatz 4 können die Vertragsparteien auch andere Arten der Strafgerichtsbarkeit nach innerstaatlichem Recht begründen.

239. Wenn Straftaten mit Hilfe eines Computersystems begangen werden, können in manchen Fällen mehrere Vertragsparteien Gerichtsbarkeit für einige oder alle Teilnehmer der Straftat innehaben. Z. B. richten sich etliche über das Internet begangene Virusattacken, Betrugshandlungen und Urheberrechtsverletzungen gegen Geschädigte in vielen Staaten. Um Doppelarbeit zu vermeiden, Zeugen unnötige Unannehmlichkeiten zu ersparen oder einen Wettstreit der Strafverfolgungsbehörden der betreffenden Staaten zu verhindern oder auf andere Weise die Wirksamkeit oder Gerechtigkeit der Verfahren zu fördern, sollen die betroffenen Vertragsparteien einander konsultieren, um den für die Strafverfolgung geeignetsten Gerichtsstand zu bestimmen. In einigen Fällen dürfte es für die betreffenden Staaten am effektivsten sein, nur einen Gerichtsstand für die Strafverfolgung zu wählen; in anderen könnte es für einen Staat am sinnvollsten sein, einige Teilnehmer der Straftat zu verfolgen, während ein oder mehrere andere Staaten weitere Beteiligte verfolgen. Nach dieser Vorschrift sind beide Lösungen zulässig. Schließlich ist die Verpflichtung zur Konsultation nicht absolut, sondern besteht nur „gegebenenfalls“. Wenn z. B. eine Vertragspartei weiß, dass die Konsultation sich erübrigt (weil ihr z. B. bestätigt wurde, dass die andere Vertragspartei nichts zu veranlassen gedenkt), oder wenn sie der Auffassung ist, dass die Konsultation ihrer Ermittlung oder ihrem Verfahren abträglich sein kann, so kann sie die Konsultation aufschieben oder ablehnen.

Kapitel III
Internationale Zusammenarbeit

240. Kapitel III enthält eine Reihe von Bestimmungen zur Auslieferung und Rechtshilfe in Strafsachen zwischen den Vertragsparteien.

Abschnitt 1 – Allgemeine Grundsätze

Titel I
Allgemeine Grundsätze der
internationalen Zusammenarbeit

Allgemeine Grundsätze der internationalen Zusammenarbeit (Artikel 23)

241. Artikel 23 enthält drei allgemeine Grundsätze der internationalen Zusammenarbeit nach Kapitel III.

242. Dieser Artikel verdeutlicht zunächst, dass die Vertragsparteien „in größtmöglichem Umfang“ untereinander auf internationaler Ebene zusammenarbeiten sollen. Dieser Grundsatz verpflichtet die Vertragsparteien, untereinander umfassend zu kooperieren und Hindernisse, die einem gleichmäßigen schnellen Fluss von Informationen und Beweisdaten entgegenstehen, auf zwischenstaatlicher Ebene auf ein Minimum zu reduzieren.

243. Darüber hinaus ist der Umfang der Verpflichtung zur Zusammenarbeit in Artikel 23 dargelegt; diese soll sich auf alle Straftaten, die Computersysteme und -daten betreffen (d. h. die in Artikel 14 Absatz 2 Buchstaben a bis b vorgesehenen Straftaten), sowie die Erhebung von Beweisen einer Straftat in elektronischer Form erstrecken. Daraus folgt, dass die Bestimmungen von Kapitel III sowohl in den Fällen, in denen die Straftat mit Hilfe eines Computersystems begangen worden ist, als auch in solchen, in denen es bei einer nicht mittels eines Computersystem begangenen gewöhnlichen Straftat (z. B. Mord) auch elektronischer Beweismittel bedarf, anwendbar sind. Es ist jedoch darauf hinzuweisen, dass

die Vertragsparteien nach den Artikeln 24 (Auslieferung), 33 (Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit) und 34 (Rechtshilfe bei der Erhebung von Inhaltsdaten in Echtzeit) im Hinblick auf diese Maßnahmen einen anderen Anwendungsbereich vorsehen können.

244. Schließlich ist die Zusammenarbeit zum einen „nach den Bestimmungen dieses Kapitels“ und zum anderen „durch Anwendung einschlägiger völkerrechtlicher Übereinkünfte über die internationale Zusammenarbeit in Strafsachen sowie Vereinbarungen, die auf der Grundlage einheitlicher oder auf gegenseitig beruhender Rechtsvorschriften getroffen wurden, und innerstaatlicher Rechtsvorschriften“ durchzuführen. Letztere Klausel schreibt den allgemeinen Grundsatz fest, dass die Bestimmungen von Kapitel III die Vorschriften der zwischenstaatlichen Rechtshilfe- und Auslieferungsübereinkommen, die zwischen den Vertragsparteien dieser Übereinkommen geschlossenen Gegenseitigkeitsabkommen (auf die in den Ausführungen zu Artikel 27 näher eingegangen wird) oder die im Hinblick auf die internationale Zusammenarbeit maßgeblichen Bestimmungen des innerstaatlichen Rechts nicht ersetzen. Dieser wesentliche Grundsatz wird in den Artikeln 24 (Auslieferung), 25 (Allgemeine Grundsätze der Rechtshilfe), 26 (Unaufgeforderte Übermittlung von Informationen), 27 (Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte), 28 (Vertraulichkeit und Beschränkung der Verwendung), 31 (Rechtshilfe beim Zugriff auf gespeicherte Computerdaten), 33 (Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit) und 34 (Rechtshilfe bei der Erhebung von Inhaltsdaten in Echtzeit) ausdrücklich bestätigt.

Titel 2
Grundsätze der Auslieferung

Auslieferung (Artikel 24)

245. In Absatz 1 heißt es, dass die Auslieferungspflicht sich nur auf die in Übereinstimmung mit den Artikeln 2 bis 11 des Übereinkommens festgelegten Straftaten bezieht, die nach den Rechtsvorschriften der beiden Vertragsparteien mit einer Freiheitsstrafe im Höchstmaß von mindestens einem Jahr oder mit einer schwereren Strafe bedroht sind. Die Verfasser haben beschlossen, eine Mindeststrafe vorzusehen, weil die Vertragsparteien nach dem Übereinkommen einige Straftaten mit einer relativ kurzzeitigen Freiheitsstrafe im Höchstmaß bedrohen können (wie z. B. im Falle von Artikel 2 – rechtswidriger Zugang – und von Artikel 4 – Eingriff in Daten). Die Verfasser hielten es demnach nicht für angebracht, das Erfordernis aufzustellen, dass jede nach den Artikeln 2 bis 11 festgelegte Straftat *ipso facto* auslieferungsfähig sein sollte. Sie haben sich also auf eine Bestimmung verständigt, wonach eine Straftat als auslieferungsfähig gilt, wenn – entsprechend dem Wortlaut des Artikels 2 des Europäischen Auslieferungsübereinkommens (ETS Nr. 24) – die Höchststrafe, die im Falle einer Straftat verhängt werden kann, derentwegen um Auslieferung ersucht wird, eine Freiheitsstrafe von mindestens einem Jahr darstellt. Ob eine Straftat nun auslieferungsfähig ist oder nicht, hängt nicht von der im Einzelfall tatsächlich verhängten Sanktion ab, sondern vielmehr von dem Höchstmaß, das von Gesetzes wegen im Falle der Straftat verhängt werden kann, derentwegen um Auslieferung ersucht wird.

246. Entsprechend dem allgemeinen Grundsatz, wonach die in Kapitel III vorgesehene internationale Zusammenarbeit gemäß den Bestimmungen der zwischen den Vertragsparteien verbindlichen Regelwerke zu erfolgen hat, sieht Absatz 1 andererseits auch vor, dass wenn ein Auslieferungsvertrag oder eine auf der Grundlage einheitlicher oder gegenseitiger Rechtsvorschriften getroffene Vereinbarung zwischen zwei oder mehreren Vertragsparteien in Kraft ist (siehe die Erläuterung dieser Formulierung in dem Kommentar zu Artikel 27 unten), die eine andere Schwelle für die Auslieferung vorsehen, die in dem Vertrag oder der Vereinigung bezeichnete Schwelle anwendbar ist. So sehen z. B. zahlreiche zwischen europäischen und nichteuropäischen Staaten geschlossene Auslieferungsverträge vor, dass eine Straftat nur dann auslieferungsfähig ist, wenn die Höchststrafe eine Freiheitsstrafe im Maße von mehr als einem Jahr oder eine schwerere Strafe ist. In solchen Fällen werden die Fachleute für Auslieferungsfragen weiterhin die in ihrer Vertragspraxis übliche Schwelle ansetzen, um zu entscheiden, ob eine Straftat auslieferungsfähig ist. Selbst nach dem Europäischen Auslieferungsübereinkommen (ETS Nr. 24) kann in Vorbehalten eine andere Mindeststrafe für die Auslieferung angegeben werden. Zwischen den Vertragsparteien des genannten Übereinkommens wird, wenn eine Vertragspartei, die einen solchen Vorbehalt gemacht hat, um Auslieferung ersucht, die im Vorbehalt angegebene Strafe berücksichtigt, um zu entscheiden, ob die Straftat auslieferungsfähig ist.

247. In Absatz 2 ist niedergelegt, dass die in Absatz 1 umschriebenen Straftaten in jedem Auslieferungsvertrag zwischen den Vertragsparteien als auslieferungsfähige Straftaten zu gelten haben und in jeden künftig zwischen ihnen zu schließenden Vertrag aufzunehmen sind. Dies bedeutet aber nicht, dass die Auslieferung jedes Mal zu bewilligen ist, wenn ein solches Ersuchen gestellt wird, sondern dass vielmehr die Möglichkeit gegeben sein muss, einem Auslieferungsersuchen wegen dieser Straftaten stattzugeben. Nach Absatz 5 können die Vertragsparteien die Auslieferung anderen Bedingungen unterwerfen.

248. Nach Absatz 3 kann eine Vertragspartei, die die Auslieferung nicht gewähren würde, weil sie mit dem ersuchenden Staat keinen Auslieferungsvertrag hat oder weil die bestehenden Verträge ein Ersuchen wegen der nach diesem Übereinkommen festgelegten Straftaten nicht abdecken, dieses Übereinkommen selbst als Grundlage für die Auslieferung des Verfolgten nehmen, auch wenn sie hierzu nicht verpflichtet ist.

249. Stützt sich eine Vertragspartei nicht auf einen Auslieferungsvertrag, sondern auf allgemeine Regelungen im Hinblick auf das Auslieferungsverfahren, ist sie nach Absatz 4 verpflichtet, die in Absatz 1 bezeichneten Straftaten als auslieferungsfähige Straftaten anzuerkennen.

250. Absatz 5 führt aus, dass die ersuchte Vertragspartei nicht zur Auslieferung verpflichtet ist, wenn sie der Auffassung ist, dass die in den anwendbaren Verträgen oder im innerstaatlichen Recht vorgesehenen Bedingungen nicht erfüllt sind. Dies ist ein weiteres Beispiel für den Grundsatz, wonach die Zusammenarbeit gemäß den Bestimmungen der zwischen den Vertragsparteien in Kraft befindlichen völkerrechtlichen Übereinkünfte, gegenseitigen Vereinbarungen oder dem innerstaatlichen Recht zu erfolgen hat. So sind beispielsweise die in dem

Europäischen Auslieferungsübereinkommen (ETS Nr. 24) und seinen Zusatzprotokollen (ETS Nr. 86 und 98) aufgeführten Bedingungen und Einschränkungen auf die Vertragsparteien dieser Vereinbarungen anwendbar, die eine Auslieferung auf dieser Grundlage ablehnen können (z. B. nach Artikel 3 des Europäischen Auslieferungsübereinkommens, wonach die Auslieferung nicht bewilligt wird, wenn die strafbare Handlung als eine politische Handlung angesehen wird oder wenn anzunehmen ist, dass das Ersuchen gestellt worden ist, um eine Person aus rassischen, religiösen, nationalen oder auf politischen Anschauungen beruhenden Erwägungen zu verfolgen oder zu bestrafen).

251. Absatz 6 enthält den Grundsatz *„aut dedere aut judicare"* (Auslieferung oder Bestrafung). Da sehr viele Staaten die Auslieferung der eigenen Staatsangehörigen ablehnen, könnten Straftäter, die im Hoheitsgebiet der Vertragspartei angetroffen werden, deren Staatsangehörigkeit sie haben, die Verantwortlichkeit für eine im Hoheitsgebiet einer anderen Vertragspartei begangenen Straftat umgehen, wenn nicht die örtlichen Behörden verpflichtet sind, Maßnahmen zu ergreifen. Nach Absatz 6 muss eine Vertragspartei, wenn eine andere Vertragspartei um Auslieferung eines Straftäters ersucht hat und diese abgelehnt worden ist, weil der Verfolgte Staatsangehöriger der ersuchten Vertragspartei ist, auf Ersuchen der ersuchenden Vertragspartei den Fall ihren zuständigen Behörden zum Zwecke der Strafverfolgung unterbreiten. Ersucht die Vertragspartei, deren Auslieferungsersuchen abgelehnt worden ist, nicht um die Übernahme der Strafverfolgung, so ist die ersuchte Vertragspartei nicht zum Einschreiten verpflichtet. Ist ferner kein Auslieferungsersuchen gestellt worden oder ist die Auslieferung aus einem anderen Grund als dem der Staatsangehörigkeit abgelehnt worden, so ist die ersuchte Vertragspartei nach diesem Absatz nicht verpflichtet, die örtlichen Behörden zwecks Strafverfolgung einzuschalten. In Absatz 6 wird außerdem gefordert, dass die Ermittlungen und das Verfahren sorgfältig betrieben werden; sie müssen genauso ernst genommen werden „wie bei jeder nach dem Recht dieser Vertragspartei vergleichbaren anderen Straftat". Die Vertragspartei unterrichtet die ersuchende Vertragspartei über das Ergebnis der Ermittlungen und des Verfahrens.

252. Damit die einzelnen Vertragsparteien wissen, an wen sie die Ersuchen um Auslieferung oder vorläufige Festnahme zu richten haben, werden die Vertragsparteien in Absatz 7 aufgefordert, dem Generalsekretär des Europarats die Bezeichnung und die Anschrift ihrer Behörden mitzuteilen, die mit der Übermittlung oder dem Empfang von Ersuchen um Auslieferung oder vorläufige Festnahme betraut sind, sofern kein Vertrag vorliegt. Die Anwendung dieser Bestimmung beschränkt sich auf den Fall, in dem kein Vertrag zwischen den betreffenden Vertragsparteien geschlossen worden ist. Liegt nämlich ein für die Vertragsparteien verbindlicher zwei- oder mehrseitiger Vertrag vor (wie ETS Nr. 24), ist diesen bekannt, an wen die Ersuchen um Auslieferung oder vorläufige Festnahme zu richten sind, wobei sich das Erfordernis eines Verzeichnisses der zuständigen Behörden erübrigt. Die Unterrichtung des Generalsekretärs hat bei der Unterzeichnung oder bei der Hinterlegung der Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde durch die Vertragspartei zu erfolgen. Hervorzuheben ist, dass die Bestimmung einer Behörde die Möglichkeit über den diplomatischen Weg nicht ausschließt.

Titel 3
Allgemeine Grundsätze der Rechtshilfe

Allgemeine Grundsätze der Rechtshilfe (Artikel 25)

253. Die allgemeinen Grundsätze für die Verpflichtung zur Rechtshilfe sind in Absatz 1 aufgeführt. Rechtshilfe ist „in größtmöglichem Umfang" zu leisten. Demnach sollte wie nach Artikel 23 („Allgemeine Grundsätze der internationalen Zusammenarbeit") die Rechtshilfe grundsätzlich umfassend sein und mögliche Hindernisse streng eingegrenzt werden. Sodann gilt wie nach Artikel 23 die Pflicht zur Rechtshilfe im Prinzip für alle Straftaten im Zusammenhang mit Computersystemen oder -daten (d. h. die Straftaten nach Artikel 14 Absatz 2 Buchstabe a und b) und bezüglich der Erhebung von Beweisen in elektronischer Form für eine Straftat. Man kam überein, die verbindliche Zusammenarbeit auf diesen umfangreichen Straftatenkatalog auszudehnen, weil es angebracht ist, die Mechanismen der internationalen Kooperation in diesen beiden Bereichen zu rationalisieren. Gleichwohl erlauben es Artikel 34 und 35 den Vertragsparteien, einen unterschiedlichen Anwendungsbereich dieser Maßnahmen vorzusehen.

254. Weitere Bestimmungen in diesem Kapitel stellen klar, dass die Verpflichtung zur Rechtshilfe allgemein den Bedingungen der anwendbaren Übereinkünfte, Gesetze und Vereinbarungen über die gegenseitige Rechtshilfe unterliegt. Nach Absatz 2 ist jede Vertragspartei verpflichtet, die rechtlichen Grundlagen zu schaffen und zu gestatten, die im restlichen Teil des Kapitels bezeichneten besonderen Formen der Zusammenarbeit zu gewähren, sofern ihre Übereinkünfte, Gesetze oder Vereinbarungen Bestimmungen dieser Art nicht bereits enthalten. Die Verfügbarkeit solcher Regelungen, insbesondere derjenigen in den Artikeln 29 bis 35 (Besondere Bestimmungen – Titel 1, 2, 3), ist für die Abwicklung einer wirksamen Zusammenarbeit bei Strafsachen wegen Computerdelikte unerlässlich.

255. Bei einigen Vertragsparteien dürfte keine Notwendigkeit bestehen, besondere gesetzgeberische Maßnahmen im Hinblick auf die Anwendung der Bestimmungen nach Absatz 2 zu treffen, weil die Regelungen völkerrechtlicher Übereinkünfte, die detaillierte Rechtshilfestrukturen schaffen, als unmittelbar geltendes Recht angesehen werden. Es wird erwartet, dass die Vertragsparteien diese Bestimmungen entweder als unmittelbar geltendes Recht betrachten, da sie bereits Rechtsvorschriften haben, die hinlänglich flexibel sind und ihnen ermöglichen, die nach diesem Kapitel geschaffenen Rechtshilfemaßnahmen zu ergreifen, oder dass sie rasch die zu diesem Zweck erforderlichen gesetzgeberischen Maßnahmen treffen werden.

256. Computerdaten gelten als äußerst flüchtig. Es genügt, einige Tasten zu drücken oder ein Automatikprogramm zu starten, um sie zu löschen, was es unmöglich macht, den Täter der Handlung zu ermitteln, oder wodurch die Beweise für seine Schuld vernichtet werden. Einige Arten von Computerdaten werden nur kurzfristig gespeichert, bevor sie gelöscht werden. In anderen Fällen können Personen oder Vermögenswerte erheblich geschädigt werden, wenn die Beweise nicht rasch erhoben werden. In solchen Eilfällen müssen Ersuchen wie

auch die Erledigung in rascher Weise erfolgen. Zielsetzung von Absatz 3 ist es demnach, die Beschleunigung des Verfahrens im Hinblick auf die Gewährleistung der Rechtshilfe zu fördern und somit zu verhindern, dass wesentliche Informationen oder Beweise verloren gehen, die möglicherweise gelöscht worden sind, bevor ein Rechtshilfeersuchen erstellt und übermittelt worden oder eine Antwort eingegangen ist. Absatz 3 stellt dies sicher, indem 1) den Vertragsparteien in dringenden Fällen gestattet wird, ein Ersuchen um Zusammenarbeit über schnelle Kommunikationsmittel zu übersenden und nicht im Wege der klassischen und wesentlich langsameren Übermittlungswege in Form von versiegeltem Schriftgut per Diplomatenpost oder auf postalischem Weg; und 2) indem der ersuchten Vertragspartei auferlegt wird, schnelle Kommunikationsmittel einzusetzen, um das Ersuchen zu erledigen. Jede Vertragspartei muss in der Lage sein, diese Maßnahme anzuwenden, sollte sie nicht bereits in ihren Verträgen, Gesetzen oder Vereinbarungen vorgesehen sein. Telefax und elektronische Post werden nur als Beispiele zitiert: jedes im Einzelfall angemessene schnelle Kommunikationsmittel kann herangezogen werden. Der technologische Fortschritt dürfte weitere schnelle Kommunikationswege bereitstellen, um Rechtshilfeersuchen weiterleiten zu können. Was die Beglaubigungs- und Sicherheitsstandards anbelangt, so könnten die Vertragsparteien im Wege einer gemeinsamen Vereinbarung die Modalitäten bei der Beglaubigung von Mitteilungen und das etwaige Erfordernis besonderer Schutzmaßnahmen festlegen (einschließlich der Kryptographie), die in besonders sensiblen Fällen als notwendig erscheinen könnten. Schließlich kann die ersuchte Vertragspartei nach diesem Absatz verlangen, dass der beschleunigten Übermittlung eine auf dem üblichen Geschäftsweg übermittelte förmliche Bestätigung folgt.

257. In Absatz 4 ist der Grundsatz verankert, wonach die Rechtshilfe den Bestimmungen der anwendbaren Rechtshilfeverträge und den innerstaatlichen Rechtsvorschriften unterliegt. Diese Regelungen stellen die Rechte der Personen sicher, die sich im Hoheitsgebiet der ersuchten Vertragspartei befinden und Gegenstand eines Rechtshilfeersuchens sein können. So wird z. B. eine eingreifende Maßnahme wie Durchsuchung und Beschlagnahme im Auftrag einer ersuchenden Vertragspartei erst dann vorgenommen, wenn die ersuchte Vertragspartei Gewissheit darüber hat, dass die erforderlichen Bedingungen für eine solche Maßnahme in einer innerstaatlichen Angelegenheit erfüllt sind. Die Vertragsparteien können ebenfalls den Schutz der Rechte von Personen in Bezug auf die im Wege der Rechtshilfe sichergestellten und herausgegebenen Sachen garantieren.

258. Der Absatz 4 ist jedoch nicht anwendbar, wenn „in diesem Kapitel nicht ausdrücklich etwas anderes vorgesehen ist“. Dieser Wortlaut soll darauf hindeuten, dass in dem Übereinkommen mehrere wichtige Abweichungen vom allgemeinen Grundsatz enthalten sind. Die erste ergibt sich aus Absatz 2 dieses Artikels, wonach jede Vertragspartei verpflichtet ist, die in den übrigen Artikeln des Kapitels aufgeführten Formen der Zusammenarbeit zu gewährleisten (wie Sicherung, Echtzeit-Erhebung von Daten, Durchsuchung und Beschlagnahme sowie Netzwerk 24/7), unabhängig davon, ob diese Maßnahmen in ihren Rechtshilfeverträgen, gleichwertigen Vereinbarungen oder Rechtsvorschriften über Rechtshilfe bereits verankert sind. Eine weitere Ausnahme findet sich in Artikel 27, der bei der Erledigung von Ersuchen stets anwendbar ist anstelle des innerstaatlichen Rechts der ersuchten Vertragspartei über die internationale Zusammenarbeit, wenn es keinen Rechtshilfevertrag und keine gleichwertige Vereinbarung zwischen der ersuchenden und der ersuchten Vertragspartei gibt. Artikel 27 enthält ein System von Bedingungen und Ablehnungsgründen. Eine weitere in Artikel 25 Absatz 4 vorgesehene Ausnahme ist, dass die Zusammenarbeit, zumindest was die Artikel 2 bis 11 des Übereinkommens angeht, nicht deshalb abgelehnt werden darf, weil die ersuchte Vertragspartei der Auffassung ist, dass sich das Ersuchen auf eine „fiskalische“ Straftat bezieht. Schließlich stellt der Artikel 29 eine Abweichung in dem Sinne dar, dass nach dem Wortlaut die Sicherung nicht aus Gründen der beiderseitigen Strafbarkeit abgelehnt werden kann, obgleich die Möglichkeit vorgesehen ist, diesbezüglich einen Vorbehalt anzubringen.

259. Absatz 5 enthält im Wesentlichen eine Definition der beiderseitigen Strafbarkeit zu Zwecken der Rechtshilfe im Sinne dieses Kapitels. Wenn es der ersuchten Vertragspartei gestattet ist, die Rechtshilfe an die Bedingung der beiderseitigen Strafbarkeit zu knüpfen (wenn sie sich z. B. das Recht vorbehalten hat, die beiderseitige Strafbarkeit als Bedingung für die Erledigung eines Ersuchens um Sicherung von Daten gemäß Artikel 29 Absatz 6 – „Beschleunigte Sicherung gespeicherter Computerdaten“ – zu verlangen), gilt diese Bedingung als erfüllt, wenn die Handlung, die der Straftat zugrunde liegt, derentwegen um Rechtshilfe ersucht wird, nach dem innerstaatlichen Recht der ersuchten Vertragspartei ebenfalls den Tatbestand einer Straftat erfüllt, selbst wenn das innerstaatliche Recht dieses Delikt einer anderen Kategorie von Straftaten zuordnet oder mit anderen Begriffsbestimmungen umschreibt. Dieser Wortlaut wurde für notwendig erachtet, um sicherzustellen, dass die ersuchten Vertragsparteien sich nicht auf ein allzu starres Kriterium berufen, wenn sie den Grundsatz der beiderseitigen Strafbarkeit anwenden. Angesichts der Unterschiede zwischen den einzelstaatlichen Rechtsordnungen dürften Abweichungen bei der Terminologie und der Einstufung krimineller Handlungen nicht verwunderlich sein. Stellt die Handlung eine Straftat in beiden Rechtsordnungen dar, dürften diese Unterschiede technischer Natur das Gewähren der Rechtshilfe wohl nicht behindern. In den Fällen, in denen das Kriterium der beiderseitigen Strafbarkeit gültig ist, sollte dieses gleichwohl in flexibler Form zur Anwendung gelangen, um das Gewähren der Rechtshilfe zu erleichtern.

Unaufgeforderte Übermittlung von Informationen (Artikel 26)

260. Dieser Artikel wurde von Bestimmungen aus früheren Rechtsinstrumenten des Europarats übernommen, wie z. B. Artikel 10 des Übereinkommens über Geldwäsche sowie Ermittlung, Beschlagnahme und Einziehung von Erträgen aus Straftaten (ETS Nr. 141) und Artikel 28 des Strafrechtsübereinkommens über Korruption (ETS Nr. 173). In zunehmendem Maße tritt die Situation ein, dass eine Vertragspartei im Besitz wertvoller Informationen ist und erwägt, dass diese für die Ermittlungen oder Verfahren von Nutzen sein könnten, die von einer anderen Vertragspartei eingeleitet oder durchgeführt werden, die aber von deren Existenz in Unkenntnis ist. In solchen Fällen dürfte kein Rechtshilfeersuchen gestellt werden.

Absatz 1 gestattet es dem Staat, der im Besitz der betreffenden Information ist, diese ohne vorheriges Ersuchen an eine andere Vertragspartei weiterzugeben. Diese Bestimmung wurde als zweckdienlich erachtet, weil nach den Rechtsvorschriften einiger Staaten eine solche positive Ermächtigung erforderlich ist, um die Rechtshilfe ohne ein Ersuchen gewähren zu können. Die Vertragsparteien sind nicht verpflichtet, anderen Vertragsparteien unaufgefordert Informationen zu erteilen, sie können dies je nach Einzelfall nach freiem Ermessen tun. Die unaufgeforderte Übermittlung von Informationen hindert die übermittelnde Vertragspartei nicht daran, sofern sie zuständig ist, bezüglich der offenbarten Tatsachen Ermittlungen anzustellen oder ein Verfahren einzuleiten.

261. In Absatz 2 wird der Umstand behandelt, dass eine Vertragspartei in bestimmten Fällen die Informationen nur dann unaufgefordert übermitteln wird, wenn die sensiblen Informationen vertraulich bleiben oder nur unter bestimmten Voraussetzungen verwendet werden. So dürfte die Vertraulichkeit von besonderer Bedeutung in den Fällen sein, in denen gewichtige Interessen des übermittelnden Staates berührt werden könnten, sollten diese Informationen in die Öffentlichkeit gelangen, wenn es z. B. notwendig ist, die Art der Informationserlangung geheim zu halten oder die Tatsache, dass eine kriminelle Vereinigung Gegenstand des Ersuchens ist. Sollte sich nach vorheriger Anfrage erweisen, dass der Empfängerstaat die von einer anderen Vertragspartei an die Verwendung der Informationen gestellte Bedingung nicht erfüllen kann (weil sie z. B. dem Gebot der Vertraulichkeit nicht nachkommen kann, da die betreffenden Informationen als Beweismittel in einem öffentlichen Verfahren benötigt werden), hat die empfangende Vertragspartei die andere zu unterrichten, die daraufhin entscheidet, ob sie diese Informationen übermittelt oder nicht. Stimmt die empfangende Vertragspartei der Bedingung jedoch zu, so ist sie daran gebunden. Man geht davon aus, dass die Bedingungen nach diesem Artikel mit denjenigen übereinstimmen dürften, die von der übermittelnden Vertragspartei auf ein Rechtshilfeersuchen der empfangenden Vertragspartei gestellt werden könnten.

Titel 4
Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte

Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte (Artikel 27)

262. Artikel 27 verpflichtet die Vertragsparteien zur Anwendung bestimmter Rechtshilfeverfahren und -bedingungen, wenn zwischen der ersuchenden und der ersuchten Vertragspartei kein Rechtshilfevertrag und keine auf einheitliche oder gegenseitige Rechtsvorschriften gestützte Vereinbarung in Kraft ist. Der Artikel bekräftigt damit den allgemeinen Grundsatz, demgemäß Rechtshilfe durch Anwendung einschlägiger Verträge oder ähnlicher Vereinbarungen über die Rechtshilfe geleistet werden sollte. Die Verfasser des Entwurfs lehnten die Schaffung einer eigenständigen allgemeinen Regelung für die Rechtshilfe, die anstelle anderer anwendbarer Übereinkünfte oder Vereinbarungen anzuwenden wäre, in diesem Übereinkommen ab, und kamen stattdessen dahingehend überein, dass es praktischer wäre, auf bestehende Rechtshilferegelungen zurückzugreifen. Dies würde es den in der Rechtshilfe tätigen Personen erlauben, die Übereinkünfte und Vereinbarungen zu nutzen, die ihnen am vertrautesten sind, und vermeiden, dass durch die Schaffung konkurrierender Regelungen möglicherweise Verwirrungen entstehen. Wie bereits erwähnt, nur bezogen auf die für eine rasche und wirksame Zusammenarbeit in computerbezogenen Strafsachen besonders erforderlichen Maßnahmen, wie sie in den Artikeln 29 bis 35 enthalten sind (Besondere Bestimmungen – Titel 1, 2 und 3), ist jede Vertragspartei verpflichtet, eine rechtliche Grundlage zur Ermöglichung derartiger Formen der Zusammenarbeit zu schaffen, wenn diese nicht bereits durch ihre bestehenden Rechtshilfeverträge, -vereinbarungen oder -vorschriften gegeben ist.

263. Daher werden die meisten Formen der in diesem Kapitel vorgesehenen Rechtshilfe weiterhin nach dem Europäischen Übereinkommen über die Rechtshilfe in Strafsachen (ETS Nr. 30) und seinem Zusatzprotokoll (ETS Nr. 99) zwischen den Vertragsparteien dieser Übereinkünfte durchgeführt werden. Alternativ können die Vertragsparteien dieses Übereinkommens, zwischen denen bilaterale Rechtshilfeverträge in Kraft sind oder die andere multilaterale Vereinbarungen über die Rechtshilfe in Strafsachen getroffen haben (wie z. B. zwischen den Mitgliedstaaten der Europäischen Union), die darin enthaltenen Bestimmungen weiterhin anwenden, ergänzt durch die besonderen, Computerstraftaten betreffenden Maßnahmen, die im übrigen Teil von Kapitel III beschrieben sind, sofern sie nicht beschließen, stattdessen die Bestimmungen dieses Artikels ganz oder teilweise anzuwenden. Die Rechtshilfe kann sich auch auf Vereinbarungen gründen, die auf der Grundlage einheitlicher oder gegenseitiger Rechtsvorschriften getroffen wurden, wie dies bei dem zwischen den nordischen Ländern entwickelten System der Zusammenarbeit, das auch in dem Europäischen Übereinkommen über die Rechtshilfe in Strafsachen (Artikel 25 Absatz 4) zugelassen ist, und zwischen Mitgliedern des Commonwealth der Fall ist. Schließlich beschränkt sich der Hinweis auf Rechtshilfeverträge oder -vereinbarungen nicht allein auf die Übereinkünfte, die zum Zeitpunkt des Inkrafttretens des vorliegenden Übereinkommens in Kraft sind, sondern deckt auch solche Übereinkünfte ab, die zukünftig verabschiedet werden könnten.

264. Artikel 27 (Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte) enthält in den Absätzen 2 bis 9 eine Reihe von Regeln für die Leistung von Rechtshilfe in Fällen, in denen kein Rechtshilfevertrag und keine auf einheitliche oder gegenseitige Rechtsvorschriften gestützte Vereinbarung in Kraft ist. Dazu gehören die Bestimmung zentraler Behörden, die Festlegung von Bedingungen, die Gründe für Ablehnung oder Aufschub und die entsprechenden Verfahren, die Vertraulichkeit von Ersuchen und die unmittelbare Übermittlung. Bezüglich dieser besonders behandelten Punkte sind, wenn es keinen Rechtshilfevertrag oder keine Vereinbarung auf der Grundlage einheitlicher oder gegenseitiger Rechtsvorschriften gibt, die Bestimmungen dieses Artikels anstelle der sonst anwendbaren innerstaatlichen Rechtsvorschriften über die Rechtshilfe anzuwenden. Andererseits werden in Artikel 27 andere Punkte, die üblicherweise in den innerstaatlichen Rechtsvorschriften über die Rechtshilfe behandelt werden, nicht geregelt. So gibt es beispielsweise keine Bestimmungen über Form und Inhalt von Ersuchen, die Zeugenvernehmung im ersuchten oder im ersuchenden Staat, die Bereitstellung amtlicher oder geschäftlicher

Unterlagen, die Überstellung inhaftierter Zeugen oder die Hilfeleistung in Beschlagnahmeangelegenheiten. Bezüglich dieser Punkte besagt Artikel 25 Absatz 4, dass die Modalitäten der Leistung dieser Art von Rechtshilfe sich nach dem Recht der ersuchten Vertragspartei richten, wenn dieses Kapitel keine besondere Bestimmung enthält.

265. Absatz 2 besagt, dass eine oder mehrere zentrale Behörden zu bestimmen sind, die den Auftrag haben, die Rechtshilfeersuchen zu übermitteln und zu beantworten. Die Schaffung zentraler Behörden ist in modernen Übereinkünften, die sich mit der Rechtshilfe in Strafsachen befassen, häufig anzutreffen und im Hinblick auf die Gewährleistung der bei der Bekämpfung von Computerstraftaten so wichtigen Schnelligkeit der Reaktion besonders nützlich. Zunächst einmal ist die unmittelbare Übermittlung zwischen solchen Behörden schneller und effizienter als die Übermittlung auf diplomatischem Wege. Zusätzlich erfüllt die Bestimmung einer aktiven zentralen Behörde eine wichtige Funktion im Hinblick darauf, dass die sorgfältige Erledigung ein- oder ausgehender Ersuchen sichergestellt wird, die jeweilige ausländische Strafvollstreckungsbehörde dahingehend beraten werden kann, wie sie die gesetzlichen Anforderungen im ersuchten Vertragsstaat am besten erfüllt, und besonders eilige oder sensible Ersuchen angemessen behandelt werden.

266. Die Vertragsparteien werden dazu ermutigt, aus Effizienzgründen eine einzige zentrale Behörde für Rechtshilfeangelegenheiten zu bestimmen. Im Allgemeinen wird es am effizientesten sein, wenn die zentrale Behörde, die nach den in dem Vertragsstaat gültigen Rechtshilfeverträgen oder nach innerstaatlichem Recht für diese Zwecke benannt wurde, auch für die Fälle, in denen die Bestimmungen dieses Artikels anzuwenden sind, zuständig ist. Eine Vertragspartei hat jedoch die Möglichkeit, mehr als eine zentrale Behörde zu bestimmen, wenn dies für ihr Rechtshilfesystem zweckmäßig ist. Wird mehr als eine zentrale Behörde bestimmt, so sollte die entsprechende Vertragspartei sicherstellen, dass jede Behörde die Bestimmungen des Übereinkommens gleich auslegt, und dass sowohl eingehende als auch ausgehende Ersuchen rasch und effizient erledigt werden. Jede Vertragspartei hat dem Generalsekretär des Europarats Namen und Anschrift (einschließlich E-Mail- und Fax-Adresse) der Behörde oder der Behörden mitzuteilen, die dazu bestimmt worden sind, Rechtshilfeersuchen nach diesem Artikel zu übermitteln und zu beantworten, und die Parteien sind dazu verpflichtet, sicherzustellen, dass diese Angaben stets auf dem aktuellen Stand sind.

267. Ein um Rechtshilfe ersuchender Staat ist oft sehr daran interessiert, sicherzustellen, dass seine innerstaatlichen Rechtsvorschriften über die Zulässigkeit von Beweismitteln eingehalten werden, damit er die Beweismittel vor Gericht auch nutzen kann. Um zu gewährleisten, dass diesen Beweisanforderungen entsprochen wird, ist die ersuchte Vertragspartei nach Absatz 3 verpflichtet, Ersuchen nach Maßgabe der von der ersuchenden Vertragspartei bezeichneten Verfahren zu erledigen, sofern dies nicht mit den Rechtsvorschriften der ersuchten Vertragspartei unvereinbar ist. In diesem Zusammenhang ist zu betonen, dass der Absatz sich nur auf die Verpflichtung zur Beachtung technischer Verfahrenserfordernisse bezieht, nicht jedoch auf grundsätzliche verfahrensrechtliche Garantien. So kann eine ersuchende Vertragspartei beispielsweise nicht von der ersuchten Vertragspartei verlangen, eine Durchsuchung und Beschlagnahme durchzuführen, die den grundlegenden gesetzlichen Voraussetzungen, welche die ersuchte Vertragspartei an eine solche Maßnahme stellt, nicht entsprechen würde. Da diese Verpflichtung also sehr begrenzt ist, wurde vereinbart, dass die bloße Tatsache, dass das Rechtssystem des ersuchten Vertragsstaats ein solches Verfahren nicht kennt, nicht Grund genug ist, die Anwendung des von dem ersuchenden Vertragsstaat erbetenen Verfahrens zu verweigern; das Verfahren muss dazu mit den Rechtsgrundsätzen der ersuchten Vertragspartei unvereinbar sein. So kann es z. B. vorkommen, dass ein Zeuge nach dem Verfahrensrecht der ersuchenden Vertragspartei unter Eid aussagen muss. Selbst wenn eine solche Aussage unter Eid nach den innerstaatlichen Bestimmungen der ersuchten Vertragspartei nicht erforderlich ist, sollte dem Ersuchen der ersuchenden Vertragspartei entsprochen werden.

268. Absatz 4 beinhaltet die Möglichkeit der Ablehnung von Rechtshilfeersuchen nach diesem Artikel. Die Rechtshilfe kann abgelehnt werden aus den in Artikel 25 Absatz 4 genannten Gründen (d. h. aus Gründen, die sich aus den Rechtsvorschriften des ersuchten Vertragsstaats ergeben), einschließlich der Beeinträchtigung der Souveränität des Staates, der Sicherheit, der öffentlichen Ordnung (ordre public) und anderer wesentlicher Interessen, und wenn es sich nach Auffassung der ersuchten Vertragspartei bei der Straftat um eine politische oder mit einer solchen zusammenhängenden Straftat handelt. Um den vorrangigen Grundsatz zu stärken, demgemäß Rechtshilfe im größtmöglichen Umfang gewährt werden sollte (Artikel 23, 25), sollten die von einer ersuchten Vertragspartei festgelegten Ablehnungsgründe eng gefasst sein und mit Zurückhaltung angewandt werden. Sie sollten nicht so umfassend sein, dass die Möglichkeit geschaffen würde, die Rechtshilfe kategorisch abzulehnen, und keinen unnötigen Bedingungen in Bezug auf umfassende Beweise oder Auskünfte unterliegen.

269. In Einklang mit dieser Betrachtungsweise wurde davon ausgegangen, dass abgesehen von den in Artikel 28 genannten Gründen die Rechtshilfe nur in Ausnahmefällen aus Datenschutzgründen abgelehnt werden kann. Eine solche Situation könnte sich ergeben, wenn die Überlassung der von der ersuchenden Vertragspartei gewünschten speziellen Daten nach Abwägung der mit dem betreffenden Fall verbundenen wichtigen Interessen (öffentliche Interessen einschließlich der geordneten Rechtspflege einerseits und Datenschutzinteressen andererseits) Probleme aufwerfen würde, die so grundlegend sind, dass sie von der ersuchten Vertragspartei als unter den Ablehnungsgrund wesentliche Interessen fallend angesehen werden müssten. Eine umfassende, kategorische oder systematische Anwendung von Datenschutzgrundsätzen zur Versagung der Zusammenarbeit ist daher ausgeschlossen. Die Tatsache, dass die beteiligten Vertragsparteien unterschiedliche Datenschutzsysteme haben (z. B. dass die ersuchende Vertragspartei keine gleichgestellte spezielle Datenschutzbehörde hat) oder über unterschiedliche Möglichkeiten zum Schutz personenbezogener Daten verfügen (z. B. dass die ersuchende Vertragspartei andere Mittel als das Verfahren der Löschung benutzt, um die Privatheit oder die Richtigkeit der von den Strafverfolgungsbehörden entgegengenommenen personenbezogenen Daten zu

schützen), stellt deshalb an sich keinen Ablehnungsgrund dar. Bevor sich die ersuchte Vertragspartei auf „wesentliche Interessen“ als Grund für die Versagung der Zusammenarbeit beruft, sollte sie zunächst versuchen, Bedingungen zu stellen, unter denen die Daten übersandt werden könnten (siehe Artikel 27 Absatz 6 und Nr. 271 dieses Berichts).

270. Absatz 5 erlaubt es der ersuchten Vertragspartei, die Rechtshilfe zwar aufzuschieben, jedoch nicht abzulehnen, wenn die unverzügliche Erledigung des Ersuchens Ermittlungen oder Verfahren im Hoheitsgebiet der ersuchten Vertragspartei beeinträchtigen würde. Möchte die ersuchende Vertragspartei beispielsweise Beweismittel oder Zeugenaussagen zu Ermittlungs- oder Verhandlungszwecken erlangen und dieselben Beweismittel oder Zeugenaussagen werden für eine Verhandlung benötigt, die im ersuchten Staat unmittelbar bevorsteht, so wäre es gerechtfertigt, dass die ersuchte Vertragspartei die Gewährung der Rechtshilfe aufschiebt.

271. In Absatz 6 ist vorgesehen, dass die ersuchte Vertragspartei in Fällen, in denen die erbetene Rechtshilfe sonst abgelehnt oder aufgeschoben werden könnte, die Gewährung der Rechtshilfe stattdessen an Bedingungen knüpfen kann. Erscheinen die Bedingungen der ersuchenden Vertragspartei nicht angemessen, so kann die ersuchte Vertragspartei sie abändern oder aber von ihrem Recht auf Ablehnung oder Aufschub der Rechtshilfe Gebrauch machen. Da die ersuchte Vertragspartei die Pflicht hat, Rechtshilfe im größtmöglichen Umfang zu gewähren, wurde vereinbart, dass sowohl mit Ablehnungsgründen als auch mit Bedingungen zurückhaltend verfahren werden sollte.

272. In Absatz 7 wird die ersuchte Vertragspartei dazu verpflichtet, die ersuchende Vertragspartei über das Ergebnis des Ersuchens zu unterrichten und eine Ablehnung oder einen Aufschub der Rechtshilfe zu begründen. Die Angabe von Gründen kann, unter anderem, der ersuchenden Vertragspartei dabei helfen, zu verstehen, wie die ersuchte Vertragspartei die Bestimmungen dieses Artikels interpretiert, die Grundlage für Beratungen mit dem Ziel der Verbesserung der Effizienz künftiger Rechtshilfe bilden und der ersuchenden Vertragspartei zuvor unbekannte faktische Informationen über Verfügbarkeit und Bedingungen von Zeugenaussagen und Beweisen liefern.

273. Manchmal stellt eine Vertragspartei ein Ersuchen in einem besonders sensiblen Fall oder in einem Fall, in dem es empfindliche Konsequenzen hätte, wenn die dem Ersuchen zugrunde liegenden Tatsachen vorzeitig öffentlich gemacht würden. Nach Absatz 8 kann die ersuchende Vertragspartei daher darum ersuchen, das Bestehen und den Inhalt des Ersuchens vertraulich zu behandeln. Diese Vertraulichkeit kann jedoch nur in dem Maße verlangt werden, wie die Möglichkeit der ersuchten Vertragspartei, die erbetenen Beweismittel oder Auskünfte zu erlangen, nicht eingeschränkt wird, wenn beispielsweise Informationen offengelegt werden müssen, um einen für die Erledigung des Ersuchens erforderlichen Gerichtsbeschluss zu erlangen, oder wenn Privatpersonen, die im Besitz von Beweismitteln sind, von dem Ersuchen in Kenntnis gesetzt werden müssen, damit es erfolgreich erledigt werden kann. Kann die ersuchte Vertragspartei der verlangten Vertraulichkeit nicht entsprechen, so setzt sie die ersuchende Vertragspartei davon in Kenntnis. Diese hat dann die Möglichkeit, das Ersuchen abzuändern oder zurückzuziehen.

274. Die nach Absatz 2 bestimmten zentralen Behörden sollen unmittelbar miteinander kommunizieren. In dringenden Fällen können Rechtshilfeersuchen jedoch von Richtern und Staatsanwälten der ersuchenden Vertragspartei unmittelbar an die Richter und Staatsanwälte der ersuchten Vertragspartei übermittelt werden. Der Richter oder Staatsanwalt, der dieses Verfahren anwendet, muss eine Abschrift des Ersuchens auch an seine eigene zentrale Behörde senden, die es dann an die zentrale Behörde der ersuchten Vertragspartei weiterleitet. Gemäß Buchstabe b können Ersuchen über Interpol übermittelt werden. Erhalten Behörden der ersuchten Vertragspartei ein Ersuchen, das nicht in ihren Zuständigkeitsbereich fällt, so haben sie gemäß Buchstabe c zwei Verpflichtungen nachzukommen. Erstens müssen sie das Ersuchen an die zuständige Behörde der ersuchten Vertragspartei weiterleiten. Zweitens müssen sie die Behörden der ersuchenden Vertragspartei über die Weiterleitung in Kenntnis setzen. Gemäß Buchstabe d können Ersuchen ohne Beteiligung der zentralen Behörden selbst dann unmittelbar übermittelt werden, wenn kein dringender Fall vorliegt, sofern die Behörde der ersuchten Vertragspartei in der Lage ist, das Ersuchen zu erledigen, ohne dabei auf Zwangsmaßnahmen zurückgreifen zu müssen. Buchstabe e schließlich erlaubt es einer Vertragspartei, den anderen Vertragsparteien über den Generalsekretär des Europarats mitzuteilen, dass unmittelbare Mitteilungen aus Effizienzgründen an die zentrale Behörde zu richten sind.

Vertraulichkeit und Beschränkung der Verwendung (Artikel 28)

275. In dieser Bestimmung wird speziell die Beschränkung der Verwendung von Informationen oder Unterlagen geregelt, um die ersuchte Vertragspartei in die Lage zu versetzen, in Fällen, in denen Informationen oder Unterlagen besonderer Geheimhaltung bedürfen, sicherzustellen, dass deren Verwendung nur darauf beschränkt wird, wofür die Rechtshilfe gewährt wird, oder dass sie nur den Strafverfolgungsbeamten des ersuchenden Vertragsstaates zugänglich gemacht werden. Diese Einschränkungen schaffen Garantien, die, unter anderem, zu Datenschutzzwecken zur Verfügung stehen.

276. Ebenso wie Artikel 27 ist auch Artikel 28 nur anwendbar, wenn kein Rechtshilfevertrag und keine Vereinbarung auf der Grundlage einheitlicher oder gegenseitiger Rechtsvorschriften zwischen der ersuchenden Vertragspartei und der ersuchten Vertragspartei in Kraft ist. Ist ein solcher Vertrag oder eine solche Vereinbarung in Kraft, so gelten deren Bestimmungen über Vertraulichkeit und Beschränkung der Verwendung anstelle der Bestimmungen dieses Artikels, sofern die Vertragsparteien nichts anderes beschließen. Diese Regelung vermeidet Überschneidungen mit bestehenden bilateralen und multilateralen Rechtshilfeverträgen und ähnlichen Vereinbarungen, wodurch die mit Rechtshilfe vertrauten Personen in die Lage versetzt werden, auch weiterhin nach der normalen, gut verständlichen Regelung zu arbeiten, und sie nicht versuchen müssen, zwei konkurrierende, möglicherweise widersprüchliche Übereinkünfte anzuwenden.

277. Absatz 2 ermöglicht es der ersuchten Vertragspartei, bei der Beantwortung eines Rechtshilfeersuchens zwei Arten von Bedingungen zu stellen. Erstens kann sie

verlangen, dass die Informationen oder die Unterlagen vertraulich behandelt werden, wenn dem Ersuchen ohne eine solche Bedingung nicht entsprochen werden könnte, was z. B. bei der vertraulich zu behandelnden Identität eines Informanten der Fall sein könnte. Es ist nicht angebracht, in Fällen, in denen die ersuchte Vertragspartei zur Leistung von Rechtshilfe verpflichtet ist, absolute Vertraulichkeit zu verlangen, da dies die ersuchende Vertragspartei häufig daran hindern würde, in einer Strafsache erfolgreich zu ermitteln oder strafrechtlich vorzugehen, z. B. durch die Verwendung der Beweismittel in einer öffentlichen Verhandlung (einschließlich der obligatorischen Offenlegung).

278. Zweitens kann die ersuchende Vertragspartei die Bereitstellung von Informationen oder Unterlagen an die Bedingung knüpfen, dass sie nicht für andere als die in dem Ersuchen genannten Ermittlungen oder Verfahren verwendet werden dürfen. Diese Bedingung findet nur Anwendung, wenn die ersuchte Vertragspartei sich ausdrücklich darauf beruft; andernfalls gibt es keine derartige Beschränkung der Verwendung durch die ersuchende Vertragspartei. In den Fällen, in denen diese Bedingung Anwendung findet, ist sichergestellt, dass Informationen und Material nur zu den in dem Ersuchen vorgesehenen Zwecken verwendet werden; die Verwendung des Materials zu anderen Zwecken ohne Einwilligung der ersuchten Vertragspartei ist dann ausgeschlossen. Die Verhandlungsführer erkannten bezüglich der Möglichkeit, die Verwendung zu beschränken, zwei Ausnahmen an; diese sind in den Bestimmungen des Absatzes implizit enthalten. Zunächst gilt nach den grundlegenden Rechtsprinzipien vieler Staaten, dass zur Verfügung gestelltes Material, welches eine beschuldigte Person entlastet, gegenüber der Verteidigung oder einer Gerichtsbehörde offengelegt werden muss. Außerdem dient das im Wege der Rechtshilfe zur Verfügung gestellte Material meist dazu, in einer Verhandlung, die normalerweise öffentlich ist, verwendet zu werden (einschließlich der obligatorischen Offenlegung). Hat eine solche Offenlegung stattgefunden, so ist das Material im Wesentlichen allgemein zugänglich geworden. In solchen Situationen ist es nicht möglich, bezüglich der Ermittlungen oder des Verfahrens, für das um Rechtshilfe ersucht wurde, Vertraulichkeit zu gewährleisten.

279. Kann die Vertragspartei, der die Informationen übermittelt werden, der auferlegten Bedingung nicht nachkommen, so muss sie dies gemäß Absatz 3 der Vertragspartei mitteilen, welche die Informationen zur Verfügung stellt. Diese kann dann von einer Übermittlung der Informationen absehen. Stimmt die Vertragspartei, welche die Informationen erhält, der Bedingung jedoch zu, so ist sie durch diese gebunden.

280. Absatz 4 besagt, dass von der ersuchenden Vertragspartei verlangt werden kann, anzugeben, welchen Gebrauch sie von den Informationen oder dem Material gemacht hat, das ihr unter einer in Absatz 2 beschriebenen Bedingung übermittelt wurde, damit die ersuchte Vertragspartei beurteilen kann, ob dieser Bedingung entsprochen wurde. Es wurde vereinbart, dass die ersuchte Vertragspartei keine allzu belastenden Nachweise verlangen dürfe, z. B. über jeden Zeitpunkt, zu dem auf das Material oder die Informationen zugegriffen wurde.

Abschnitt 2 – Besondere Bestimmungen

281. Dieser Abschnitt dient dazu, besondere Verfahren zu schaffen, die es ermöglichen sollen, in Fällen, die Computerstraftaten oder in elektronischer Form vorliegendes Beweismaterial betreffen, auf internationaler Ebene gemeinsam und wirkungsvoll vorzugehen.

Titel 1
Rechtshilfe bei vorläufigen Maßnahmen

Umgehende Sicherung gespeicherter Computerdaten (Artikel 29)

282. Dieser Artikel sieht ein Verfahren auf internationaler Ebene vor, das dem in Artikel 16 für die innerstaatliche Ebene vorgesehenen Verfahren entspricht. Nach Absatz 1 dieses Artikels kann eine Vertragspartei darum ersuchen, dass Daten, die im Hoheitsgebiet der ersuchten Vertragspartei mittels eines Computersystems gespeichert sind, umgehend sichergestellt werden, und nach Absatz 3 ist jede Vertragspartei zur Schaffung der gesetzlichen Voraussetzungen dafür verpflichtet. Dadurch soll vermieden werden, dass diese Daten während des Zeitraums, der für die Vorbereitung, Übermittlung und Erledigung eines Rechtshilfeersuchens um Erlangung dieser Daten erforderlich ist, verändert, entfernt oder gelöscht werden. Die Sicherstellung stellt eine begrenzte, vorläufige Maßnahme dar, die viel schneller durchzuführen ist als eine traditionelle Rechtshilfehandlung. Wie bereits erörtert, sind Computerdaten in hohem Maße flüchtig. Durch Drücken einiger weniger Tasten oder durch den Einsatz automatischer Programme können sie gelöscht, verändert oder an eine andere Stelle verbracht werden. Dadurch könnte die Zurückverfolgung einer Straftat bis zum Täter unmöglich gemacht werden oder es könnte ein entscheidender Schuldbeweis zerstört werden. Einige Formen von Computerdaten werden nur für einen kurzen Zeitraum gespeichert, bevor sie gelöscht werden. Daher kam man überein, dass ein Verfahren erforderlich sei, mit dem die Verfügbarkeit solcher Daten bis zum Abschluss des langwierigeren und komplizierteren Verfahrens der Erledigung eines förmlichen Rechtshilfeersuchens, das Wochen oder Monate in Anspruch nehmen kann, sichergestellt werden kann.

283. Diese Maßnahme ist sehr viel schneller durchzuführen als eine gewöhnliche Rechtshilfehandlung und stellt gleichzeitig einen geringeren Eingriff dar. Die mit der Rechtshilfe betrauten Beamten der ersuchten Vertragspartei müssen die Daten nicht von ihrem Verwahrer in Besitz nehmen. Bevorzugt wird eine Vorgehensweise, bei der die ersuchte Vertragspartei sicherstellt, dass der Verwahrer (häufig ein Diensteanbieter oder eine andere Drittpartei) die Daten sichert (d. h. nicht löscht), solange die Verfügung, aufgrund derer die Daten zu einem späteren Zeitpunkt an Strafverfolgungsbeamte zu übergeben sein werden, noch nicht erlassen ist. Der Vorteil dieses Verfahrens liegt sowohl in seiner Schnelligkeit als auch darin, dass es die Privatsphäre der Person schützt, auf die sich die Daten beziehen, da die Daten nicht offengelegt oder von einem Amtsträger überprüft werden, solange die Kriterien für eine vollständige Offenlegung gemäß den üblichen Rechtshilferegeln nicht erfüllt sind. Gleichzeitig wird der ersuchten Vertragspartei erlaubt, andere Verfahren zur beschleunigten Sicherung von Daten, einschließlich des beschleunigten Erlasses eines Herausgabe- oder Durchsuchungsbeschlusses bezüglich der

Daten, anzuwenden. Gefordert wird im Wesentlichen, dass ein extrem schnelles Verfahren zur Verfügung steht, durch das verhindert werden kann, dass Daten unwiederbringlich verloren sind.

284. In Absatz 2 wird der Inhalt eines gemäß diesem Artikel gestellten Ersuchens um Sicherung aufgeführt. In Anbetracht dessen, dass es sich um eine vorläufige Maßnahme handelt und das Ersuchen rasch zu verfassen und zu übermitteln ist, wird es nur solche, kurz gefassten, Angaben enthalten, die zur Sicherung der Daten unbedingt erforderlich sind. Neben der Angabe der um Sicherung ersuchenden Behörde und der Straftat, die der Maßnahme zugrunde liegt, muss das Ersuchen eine kurze Sachverhaltsdarstellung, die zur Erkennung der zu sichernden Daten und des Ortes, an dem sie sich befinden, erforderlichen Angaben sowie eine Erklärung darüber enthalten, weshalb die Daten für die Untersuchung oder Verfolgung der betreffenden Straftat benötigt werden und eine Sicherung erforderlich ist. Schließlich muss die ersuchende Vertragspartei erklären, dass sie ein Rechtshilfeersuchen um Herausgabe der Daten nachreichen wird.

285. Absatz 3 enthält den Grundsatz, dass die beiderseitige Strafbarkeit keine Voraussetzung für die Vornahme der Sicherung ist. Im Allgemeinen ist die Anwendung des Grundsatzes der beiderseitigen Strafbarkeit im Zusammenhang mit einer Sicherung kontraproduktiv. Erstens ist im Hinblick auf die moderne Rechtshilfepraxis festzustellen, dass der Trend dahin geht, die Voraussetzung der beiderseitigen Strafbarkeit nur noch für die am stärksten in die Privatsphäre eingreifenden Maßnahmen wie Durchsuchung und Beschlagnahme sowie Erhebung bestehen zu lassen. Die Sicherung stellt, so wie sie von den Verfassern des Entwurfs vorgesehen ist, jedoch keine besonders eingreifende Maßnahme dar, da der Verwahrer lediglich Daten, die sich rechtmäßig in seinem Besitz befinden, weiterhin in seinem Besitz behält, und die Daten gegenüber Amtsträgern der ersuchten Vertragspartei nicht offengelegt und nicht von diesen geprüft werden, bevor nicht einem förmlichen Rechtshilfeersuchen um Offenlegung der Daten stattgegeben worden ist. Zweitens ist, in praktischer Hinsicht, zu bemerken, dass die zur Feststellung der beiderseitigen Strafbarkeit erforderlichen Klarstellungen oft so viel Zeit in Anspruch nehmen, dass die Daten in der Zwischenzeit gelöscht, entfernt oder verändert wären. Beispielsweise kann es vorkommen, dass die ersuchende Vertragspartei im frühen Stadium einer Ermittlung feststellt, dass auf einen in ihrem Hoheitsgebiet belegenen Computer unerlaubt Zugriff genommen wurde, Art und Ausmaß des Schadens aber vielleicht erst später wirklich erkennt. Würde die ersuchte Vertragspartei die Sicherung von Verkehrsdaten, aufgrund derer das unbefugte Eindringen bis zu seinem Ursprung zurückverfolgt werden kann, bis zur eindeutigen Feststellung der beiderseitigen Strafbarkeit aufschieben, so wären diese kritischen Daten von den Diensteanbietern, die solche Daten nach der Übertragung nur für Stunden oder Tage speichern, oft bereits routinemäßig gelöscht. Selbst wenn die ersuchende Vertragspartei danach in der Lage wäre, die beiderseitige Strafbarkeit festzustellen, könnten die entscheidenden Verkehrsdaten nicht wiedererlangt werden, und der Täter würde nie ermittelt.

286. Daher gilt die allgemeine Regel, dass die Vertragsparteien auf das Erfordernis der beiderseitigen Strafbarkeit im Hinblick auf die Sicherung verzichten müssen. Nach Absatz 4 steht jedoch ein begrenzter Vorbehalt zur Verfügung. Verlangt eine Vertragspartei die beiderseitige Strafbarkeit als Voraussetzung für die Gewährung von Rechtshilfe um Herausgabe von Daten und hat sie Grund zu der Annahme, dass zum Zeitpunkt der Offenlegung die beiderseitige Strafbarkeit nicht nachgewiesen sein wird, so kann sie sich das Recht vorbehalten, die Sicherung an die Voraussetzung der beiderseitigen Strafbarkeit zu knüpfen. In Bezug auf die nach den Artikeln 2 bis 11 festgelegten Straftaten wird angenommen, dass die Voraussetzung der beiderseitigen Strafbarkeit ohnehin von den Vertragsparteien erfüllt wird, vorbehaltlich der Vorbehalte, die sie möglicherweise zu diesen Straftaten gemacht haben, soweit das Übereinkommen dies erlaubt. Daher können die Vertragsparteien diese Voraussetzung nur in Bezug auf andere als im Übereinkommen definierte Straftaten vorsehen.

287. Im Übrigen kann die ersuchte Vertragspartei gemäß Absatz 5 ein Sicherungsersuchen nur dann ablehnen, wenn seine Erledigung die nationale Souveränität, die nationale Sicherheit, die öffentliche Ordnung (ordre public) oder andere wesentliche Interessen beeinträchtigen würde, oder wenn sie die betreffende Straftat als eine politische oder als eine mit einer solchen zusammenhängenden Straftat ansieht. Aufgrund der zentralen Bedeutung dieser Maßnahme für die wirksame Untersuchung und Verfolgung von Computerstraftaten wurde vereinbart, jedwede andere Begründung für die Ablehnung eines Sicherungsersuchens auszuschließen.

288. Manchmal wird die ersuchte Vertragspartei feststellen, dass der Verwahrer der Daten wahrscheinlich etwas unternehmen wird, was die Vertraulichkeit der von der ersuchenden Vertragspartei geführten Ermittlungen gefährdet oder ihnen in anderer Weise schaden könnte (z. B. wenn die zu sichernden Daten von einem Diensteanbieter gespeichert sind, der von einer kriminellen Gruppierung kontrolliert wird oder selbst Gegenstand der Ermittlungen ist). In solchen Fällen ist nach Absatz 6 die ersuchende Vertragspartei umgehend hiervon in Kenntnis zu setzen, damit sie einschätzen kann, ob sie das mit der Aufrechterhaltung des Sicherungsersuchens verbundene Risiko eingehen oder sich um eine eingreifendere, jedoch sicherere Form der Rechtshilfe bemühen sollte, beispielsweise um eine Herausgabe oder Durchsuchung und Beschlagnahme.

289. Schließlich ist gemäß Absatz 7 jede Vertragspartei verpflichtet, sicherzustellen, dass die nach diesem Artikel gesicherten Daten bis zum Eingang eines förmlichen Rechtshilfeersuchens um Weitergabe der Daten für zunächst mindestens 60 Tage erhalten bleiben und nach Eingang des Ersuchens weiterhin gesichert werden.

Umgehende Weitergabe gesicherter Verkehrsdaten (Artikel 30)

290. Dieser Artikel stellt das internationale Gegenstück zu der in Artikel 17 für die innerstaatliche Ebene vorgesehene Befugnis dar. Häufig wird auf Ersuchen einer Vertragspartei, in deren Hoheitsgebiet eine Straftat verübt wurde, die ersuchte Vertragspartei Verkehrsdaten betreffend eine über ihre Computer gelaufene Übertragung sichern, damit die Übertragung bis zu ihrem Ursprung zurückverfolgt und der Täter identifiziert oder entscheidendes Beweismaterial lokalisiert werden kann. Dabei kann es vorkommen, dass die ersuchte Vertragspartei feststellt, dass in ihrem Hoheitsgebiet gefundene Ver-

kehrsdaten ergeben, dass die Übermittlung von einem Diensteanbieter in einem dritten Staat oder von einem Diensteanbieter in dem ersuchenden Staat selbst ausgegangen ist. In diesem Fall muss die ersuchte Vertragspartei der ersuchenden Vertragspartei schnell eine ausreichende Menge von Verkehrsdaten zur Verfügung stellen, damit der Diensteanbieter in dem anderen Staat und der Übertragungsweg aus diesem anderen Staat ermittelt werden können. Hatte die Übertragung ihren Ursprung in einem dritten Staat, so wird es der ersuchenden Vertragspartei durch diese Auskunft ermöglicht, ein Ersuchen um Sicherung und beschleunigte Rechtshilfe an diesen anderen Staat zu stellen, damit sie die Übertragung bis zu ihrem Ursprung zurückverfolgen kann. Führt der Übertragungsweg zurück zu dem ersuchenden Staat, so wird dieser in die Lage versetzt, die Sicherung und Weitergabe weiterer Verkehrsdaten mittels innerstaatlicher Verfahren zu erlangen.

291. Nach Absatz 2 kann die ersuchte Vertragspartei die Weitergabe von Verkehrsdaten nur dann ablehnen, wenn durch die Weitergabe ihre nationale Souveränität, ihre nationale Sicherheit, ihre öffentliche Ordnung (ordre public) oder andere wesentliche Interessen gefährdet würden, oder wenn sie der Auffassung ist, dass es sich bei der Straftat um eine politische oder um eine mit einer solchen zusammenhängende Straftat handelt. Ebenso wie in Artikel 29 (umgehende Sicherung gespeicherter Computerdaten) ist aufgrund der zentralen Bedeutung dieser Art von Informationen für die Ermittlung der Personen, die Straftaten im Sinne dieses Übereinkommens verübt haben, oder die Lokalisierung von äußerst wichtigem Beweismaterial eine Ablehnung auch hier nur aus eng eingegrenzten Gründen möglich, und es wurde vereinbart, jedwede andere Begründung für die Ablehnung der Rechtshilfe auszuschließen.

Titel 2
Rechtshilfe in Bezug auf Ermittlungsbefugnisse

Rechtshilfe beim Zugriff auf gespeicherte Computerdaten (Artikel 31)

292. Jede Vertragspartei muss in der Lage sein, für eine andere Vertragspartei Daten, die mittels eines Computersystems gespeichert sind, die sich in ihrem Hoheitsgebiet befinden, zu durchsuchen oder in ähnlicher Weise auf sie zuzugreifen, sie zu beschlagnahmen oder in ähnlicher Weise sicherzustellen und sie weiterzugeben – genau so, wie sie nach Artikel 19 (Durchsuchung und Beschlagnahme gespeicherter Computerdaten) in der Lage sein muss, dies zu innerstaatlichen Zwecken zu tun. Nach Absatz 1 darf eine Vertragspartei um diese Art von Rechtshilfe ersuchen, und nach Absatz 2 muss die ersuchte Vertragspartei in der Lage sein, diese zu gewähren. Absatz 2 trägt auch dem Grundsatz Rechnung, wonach eine solche Zusammenarbeit sich nach den Bedingungen richtet, die in den anzuwendenden Verträgen, Vereinbarungen und innerstaatlichen Rechtsvorschriften über die Rechtshilfe in Strafsachen enthalten sind. Nach Absatz 3 ist das Ersuchen beschleunigt zu erledigen, wenn (1) Gründe zu der Annahme vorliegen, dass bei den einschlägigen Daten eine besondere Gefahr des Verlusts oder der Veränderung besteht, oder (2) die genannten Verträge, Vereinbarungen oder Rechtsvorschriften dies vorsehen.

Grenzüberschreitender Zugriff auf gespeicherte Computerdaten mit Zustimmung oder wenn diese öffentlich zugänglich sind (Artikel 32)

293. Die Frage, wann es einer Vertragspartei erlaubt sein sollte, einseitig auf im Hoheitsgebiet einer anderen Vertragspartei gespeicherte Daten zuzugreifen, ohne um Rechtshilfe zu ersuchen, wurde von den Verfassern des Übereinkommens ausführlich diskutiert. Man beriet detailliert sowohl über solche Fälle, in denen akzeptiert werden könnte, dass Staaten einseitig handeln, als auch über Fälle, in denen dies nicht hingenommen werden könnte. Die Verfasser entschieden letztlich, dass es noch nicht möglich sei, eine umfassende, rechtsverbindliche Regelung für diesen Bereich zu schaffen. Dies lässt sich zum Teil mit dem Mangel an konkreter Erfahrung mit solchen Situationen erklären und zum Teil mit der Auffassung, dass die geeignete Lösung oft von den genauen Umständen des einzelnen Falles abhänge und es deshalb schwierig sei, allgemeine Regeln aufzustellen. Schließlich entschieden die Verfasser, in Artikel 32 des Übereinkommens nur solche Situationen aufzuführen, bezüglich derer alle der Auffassung waren, dass eine einseitige Vorgehensweise akzeptierbar sei. Sie vereinbarten, andere Fälle erst dann zu regeln, wenn weitergehende Erfahrungen gesammelt worden seien, in Anbetracht derer man erneut diskutieren könnte. Diesbezüglich ist auf Artikel 39 Absatz 3 Bezug zu nehmen, in dem bezüglich anderer Situationen weder eine Genehmigung noch ein Ausschluss vorgesehen ist.

294. In Artikel 32 (Grenzüberschreitender Zugriff auf gespeicherte Computerdaten mit Zustimmung oder wenn diese öffentlich zugänglich sind) ist von zwei Fällen die Rede: Im ersten sind die Daten, auf die zugegriffen wird, öffentlich zugänglich, und im zweiten empfängt eine Vertragspartei mittels eines Computersystems in ihrem Hoheitsgebiet Daten, die sich außerhalb ihres Hoheitsgebiets befinden, oder nimmt auf diese Zugriff, wobei sie die rechtmäßige und freiwillige Zustimmung der Person einzuholen hat, die rechtmäßig befugt ist, der Vertragspartei diese Daten mittels dieses Systems zu übermitteln. Wer eine zur Weitergabe von Daten „rechtmäßig befugte“ Person ist, kann je nach den Umständen, der Art der Person und dem jeweils anwendbaren Recht unterschiedlich sein. So kann z. B. die elektronische Post einer Person von einem Diensteanbieter in einem anderen Land gespeichert werden, oder eine Person kann Daten absichtlich in einem anderen Land speichern. Diese Personen können die Daten abrufen und, soweit sie dazu rechtmäßig befugt sind, freiwillig an Strafverfolgungsbeamte weitergeben oder diesen Beamten erlauben, auf die Daten zuzugreifen, wie in dem Artikel vorgesehen.

Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit (Artikel 33)

295. In vielen Fällen können Ermittler nicht gewährleisten, dass sie eine Kommunikation anhand der Spur von Aufzeichnungen früherer Übertragungen bis zu ihrem Ursprung zurückverfolgen können, da wichtige Verkehrsdaten vielleicht automatisch von einem Diensteanbieter in der Übertragungskette gelöscht wurden, bevor sie gesichert werden konnten. Daher ist für die Ermittler beider Vertragsparteien von entscheidender Bedeutung, dass sie Verkehrsdaten in Bezug auf Kommunikationen, die über ein Computersystem in einem anderen Vertragsstaat übertragen werden, in Echtzeit erhalten können.

Daher ist nach Artikel 33 (Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit) jede Vertragspartei verpflichtet, Verkehrsdaten für eine andere Vertragspartei in Echtzeit zu erheben. Dieser Artikel verpflichtet die Vertragsparteien, in diesem Bereich zusammenzuarbeiten, jedoch sind hier wie auch an anderer Stelle bestehende Modalitäten der Rechtshilfe zu beachten. Daher richten sich die Bedingungen einer solchen Zusammenarbeit im Allgemeinen nach den in den anwendbaren Verträgen, Vereinbarungen und Rechtsvorschriften über die Rechtshilfe in Strafsachen enthaltenen Bestimmungen.

296. In vielen Ländern wird Rechtshilfe bei der Echtzeit-Erhebung von Verkehrsdaten großzügig geleistet, da eine solche Erhebung als weniger eingreifend angesehen wird als die Erhebung von Inhaltsdaten oder die Durchsuchung und Beschlagnahme. Einige Staaten haben hier jedoch einen engeren Ansatz. So wie die Vertragsparteien nach Artikel 14 (Geltungsbereich verfahrensrechtlicher Bestimmungen) in Bezug auf den Geltungsbereich der entsprechenden innerstaatlichen Maßnahme einen Vorbehalt machen können, wird daher in Absatz 2 den Vertragsparteien gestattet, diese Maßnahme auf eine enger gefasste Reihe von Straftaten als in Artikel 23 (Allgemeine Grundsätze der internationalen Zusammenarbeit) vorgesehen zu beschränken. Es wird eine Einschränkung gemacht: die Reihe der Straftaten darf auf keinen Fall enger gefasst sein als diejenige, für die eine solche Maßnahme in einem gleichartigen inländischen Fall zur Verfügung steht. Da die Echtzeit-Erhebung von Verkehrsdaten manchmal die einzige Möglichkeit ist, die Identität eines Straftäters zu ermitteln, und weniger eingreifend ist, soll die Formulierung „zumindest“ in Absatz 2 die Vertragsparteien dazu bewegen, Rechtshilfe in größtmöglichem Umfang zu leisten, d. h. selbst ohne beiderseitige Strafbarkeit.

Rechtshilfe bei der Erhebung von Inhaltsdaten in Echtzeit (Artikel 34)

297. Da es sich beim Abfangen um eine stark in die Privatsphäre eingreifende Maßnahme handelt, ist die Verpflichtung, Rechtshilfe bei der Erhebung von Inhaltsdaten zu leisten, eingeschränkt. Die Verpflichtung beschränkt sich auf das in den anwendbaren Verträgen und Rechtsvorschriften der Vertragsparteien erlaubte Maß. Da es sich bei der Zusammenarbeit bei der Erhebung von Inhalten um einen neu entstehenden Bereich der Rechtshilfepraxis handelt, wurde beschlossen, bestehenden Rechtshilferegelungen und innerstaatlichen Rechtsvorschriften in Bezug auf das Ausmaß und die Beschränkung der Verpflichtung zur Rechtshilfe Vorrang einzuräumen. Diesbezüglich wird auf die Erläuterungen zu den Artikeln 14, 15 und 21 sowie auf das Dokument Nr. R (85) 10 betreffend die praktische Anwendung des Europäischen Übereinkommens über die Rechtshilfe in Strafsachen auf Rechtshilfeersuchen um Überwachung des Fernmeldeverkehrs verwiesen.

Titel 3
Netzwerk 24/7

24/7 - Netzwerk (Artikel 35)

298. Wie bereits erörtert wurde, ist für die wirksame Bekämpfung von Straftaten, die mittels eines Computersystems begangen wurden, sowie für die wirksame Erhebung von Beweisen in elektronischer Form eine sehr schnelle Reaktion erforderlich. Darüber hinaus kann durch das Drücken einiger weniger Tasten in einem Teil der Welt eine Handlung ausgelöst werden, deren Folgen in einer Entfernung von Tausenden von Kilometern und vielen Zeitzonen unverzüglich zu spüren sind. Aus diesem Grund werden für die bestehende polizeiliche Zusammenarbeit und bestehende Rechtshilfemodalitäten zusätzliche Verbindungswege benötigt, damit den Herausforderungen des Computerzeitalters wirksam begegnet werden kann. Der nach diesem Artikel geschaffene Verbindungsweg gründet sich auf die Erfahrungen aus einem bereits funktionierenden Netzwerk, das unter der Schirmherrschaft der G8-Staatengruppe geschaffen wurde. Nach diesem Artikel ist jede Vertragspartei verpflichtet, eine Kontaktstelle zu bestimmen, die an sieben Wochentagen 24 Stunden täglich in Anspruch genommen werden kann, damit gewährleistet ist, dass bei Ermittlungen und Verfahren nach diesem Kapitel unverzüglich Unterstützung gewährt werden kann, insbesondere im Hinblick auf die in Artikel 35 Absatz 1 Buchstaben a bis c genannten Maßnahmen. Man war sich einig, dass die Errichtung dieses Netzwerks zu den wichtigsten in diesem Übereinkommen vorgesehenen Mitteln zählt, durch die sichergestellt werden soll, dass die Vertragsparteien den Herausforderungen im Hinblick auf Computerstraftaten wirksam begegnen können.

299. Die Kontaktstelle 24/7 jeder Vertragspartei hat unter anderem die fachliche Beratung, die Sicherung von Daten, das Erheben von Beweisen, das Erteilen von Rechtsauskünften und das Ausfindigmachen verdächtiger Personen zu ermöglichen oder selbst durchzuführen. Der in Absatz 1 verwendete Begriff „Rechtsauskünfte“ bedeutet, dass eine andere Vertragspartei, die um Zusammenarbeit ersucht, im Hinblick darauf beraten wird, welche rechtlichen Voraussetzungen erfüllt sein müssen, damit eine informelle oder formelle Zusammenarbeit erfolgen kann.

300. Es steht jeder Vertragspartei frei, zu bestimmen, wo sie die Kontaktstelle in ihrem Strafverfolgungssystem ansiedelt. Vielleicht wollen einige Staaten die Kontaktstelle 24/7 in ihrer zentralen Behörde für Rechtshilfe unterbringen. Andere wiederum sind vielleicht der Auffassung, dass es am besten wäre, sie würde sich bei einer auf die Bekämpfung von Computerkriminalität spezialisierten Polizeieinheit befinden, und es gibt weitere Möglichkeiten je nach der Regierungsstruktur und dem Rechtssystem der jeweiligen Vertragspartei. Da die Kontaktstelle 24/7 sowohl fachlichen Rat zur Abwehr oder Zurückverfolgung eines Angriffs erteilen soll als auch Aufgaben wie das Ausfindigmachen von Verdächtigen im Rahmen der internationalen Zusammenarbeit erfüllen soll, gibt es nicht nur eine richtige Antwort. Es wird davon ausgegangen, dass sich die Struktur des Netzwerks mit der Zeit herausbilden wird. Bei der Bestimmung der nationalen Kontaktstelle sollte bedacht werden, dass mit Kontaktstellen kommuniziert werden muss, die andere Sprachen benutzen.

301. In Paragraph 2 ist vorgesehen, dass die Kontaktstelle 24/7 neben den anderen von ihr zu erfüllenden wichtigen Aufgaben sicherstellen soll, dass diejenigen Aufgaben, die sie nicht selbst direkt erledigen kann, rasch ausgeführt werden. Wenn die Kontaktstelle einer Vertragspartei beispielsweise Teil einer Polizeieinheit ist, so muss es ihr möglich sein, sich unverzüglich mit anderen ihrer Regierung zugehörigen zuständigen Dienststellen, wie beispielsweise der zentralen Behörde für die

Auslieferung oder die Rechtshilfe, abzustimmen, damit zu jeder Tages- und Nachtzeit die geeigneten Maßnahmen ergriffen werden können. Darüber hinaus muss die Kontaktstelle 24/7 jeder Vertragspartei in der Lage sein, sich mit anderen Mitgliedern des Netzwerks im beschleunigten Verfahren zu verständigen.

302. Nach Absatz 3 muss jede Kontaktstelle innerhalb des Netzwerks über eine geeignete Ausstattung verfügen. Moderne Telefon-, Fax- und Computeranlagen sind für den reibungslosen Betrieb des Netzwerks unerlässlich, und andere Kommunikationswege und analytische Geräte werden mit fortschreitender Technologisierung dazugehören müssen. Absatz 3 besagt auch, dass das Personal, das zum Netzwerk-Team einer Vertragspartei gehört, im Hinblick auf die Computerkriminalität und ihre wirksame Bekämpfung angemessen geschult sein muss.

Kapitel IV
Schlussbestimmungen

303. Bis auf wenige Ausnahmen beruhen die Bestimmungen in diesem Kapitel überwiegend auf den „Muster-Schlussklauseln für im Rahmen des Europarats geschlossene Übereinkommen“, die vom Ministerkomitee bei der 315. Tagung der Ministerbeauftragten im Februar 1980 genehmigt wurden. Da die Artikel 36 bis 48 in ihrer Mehrzahl in den Standardformulierungen der Musterklauseln abgefasst sind oder auf der langjährigen Vertragspraxis des Europarats basieren, bedürfen sie keiner besonderen Erläuterung. Bestimmte Abweichungen von den Musterklauseln bzw. einige neue Bestimmungen sind jedoch erläuterungsbedürftig. Es wird in diesem Zusammenhang darauf hingewiesen, dass die Musterklauseln als unverbindlicher Katalog von Bestimmungen angenommen wurden. Wie der Einführung zu den Musterklauseln zu entnehmen ist, „sind diese Muster-Schlussklauseln nur dazu bestimmt, die Aufgabe der Sachverständigenausschüsse zu erleichtern und redaktionelle Unterschiede zu vermeiden, die nicht sachlich begründet sind“. Der Musterwortlaut ist in keiner Weise verbindlich, und es können in besonderen Fällen andere Klauseln verwendet werden.

Unterzeichnung und Inkrafttreten (Artikel 36)

304. Artikel 36 Absatz 1 geht auf mehrere Vorläufer zurück, die in anderen im Rahmen des Europarats erarbeiteten Übereinkommen enthalten sind, z. B. im Übereinkommen über die Überstellung verurteilter Personen (ETS Nr. 112) und im Übereinkommen über Geldwäsche sowie Ermittlung, Beschlagnahme und Einziehung von Erträgen aus Straftaten (ETS Nr. 141); danach können nicht nur Mitgliedstaaten des Europarats, sondern auch Nichtmitgliedstaaten, die sich an der Ausarbeitung beteiligt haben, das Übereinkommen vor dem Inkrafttreten unterzeichnen. Mit dieser Bestimmung soll erreicht werden, dass möglichst viele interessierte Staaten, nicht nur Mitglieder des Europarats, so rasch wie möglich Vertragspartei werden können. Hier soll die Bestimmung auf vier Nichtmitgliedstaaten Anwendung finden – Japan, Kanada, Südafrika und die Vereinigten Staaten von Amerika – , die sich aktiv an der Ausarbeitung des Übereinkommens beteiligt haben. Nach Inkrafttreten des Übereinkommens gemäß Absatz 3 können andere Nichtmitgliedstaaten, auf die diese Bestimmung nicht anwendbar ist, eingeladen werden, dem Übereinkommen nach Artikel 37 Absatz 1 beizutreten.

305. Nach Artikel 36 Absatz 3 sind als Voraussetzung für das Inkrafttreten des Übereinkommens fünf Ratifikationen, Annahmen oder Genehmigungen vorgesehen. Diese Zahl ist größer als in den Übereinkommen des Europarats sonst üblich (drei) und spiegelt die Auffassung wider, dass eine etwas größere Staatengruppe nötig ist, um das Problem der internationalen Computerkriminalität erfolgreich anzugehen. Die Zahl ist jedoch nicht so hoch angesetzt, dass sich das Inkrafttreten des Übereinkommens unnötig verzögern würde. Unter den fünf ersten Staaten müssen zwar mindestens drei Mitgliedstaaten des Europarats sein, aber die beiden anderen könnten aus der Gruppe der vier Nichtmitgliedstaaten kommen, die sich an der Ausarbeitung des Übereinkommens beteiligt haben. Nach dieser Bestimmung könnte das Übereinkommen natürlich auch in Kraft treten, wenn fünf Mitgliedstaaten des Europarats ihre Zustimmung ausdrücken, durch das Übereinkommen gebunden zu sein.

Beitritt zum Übereinkommen (Artikel 37)

306. Artikel 37 ist ebenfalls anhand von Vorläufern in anderen Europaratsübereinkommen formuliert worden, enthält aber ein weiteres ausdrückliches Element. Der langjährigen Praxis entsprechend beschließt das Ministerkomitee von sich aus oder auf Antrag, einen Nichtmitgliedstaat, der sich nicht an der Ausarbeitung eines Übereinkommens beteiligt hat, zum Beitritt zu dem Übereinkommen einzuladen, nachdem es alle Vertragsparteien konsultiert hat, gleichviel, ob sie Mitgliedstaaten sind oder nicht. Dies bedeutet, dass das Ministerkomitee, wenn eine Vertragspartei sich gegen den Beitritt eines Nichtmitgliedstaats ausspricht, diesen in der Regel nicht einlädt, sich dem Übereinkommen anzuschließen. Nach der üblichen Formulierung könnte das Ministerkomitee jedoch – theoretisch – diesen Nichtmitgliedstaat auch dann einladen, einem Übereinkommen beizutreten, wenn eine Vertragspartei, die Nichtmitgliedstaat ist, sich gegen seinen Beitritt ausspricht. Dies bedeutet, dass in dem Verfahren der Ausdehnung von Europaratsübereinkünften auf Nichtmitgliedstaaten – theoretisch – den Vertragsparteien, die Nichtmitgliedstaaten sind, ein Vetorecht in der Regel nicht eingeräumt wird. Es ist aber ausdrücklich vorgesehen worden, dass das Ministerkomitee alle Vertragsstaaten – und nicht nur die Mitglieder des Europarats – zu konsultieren und deren einhellige Zustimmung einzuholen hat, bevor es einen Nichtmitgliedstaat zum Beitritt zu dem Übereinkommen einlädt. Wie bereits dargelegt wurde, entspricht dieses Erfordernis der Praxis und der Erkenntnis, dass es allen Vertragsstaaten des Übereinkommens möglich sein sollte zu bestimmen, mit welchen Nichtmitgliedstaaten sie ein Vertragsverhältnis eingehen. Der formelle Beschluss, einen Nichtmitgliedstaat zum Beitritt einzuladen, wird jedoch in Übereinstimmung mit der üblichen Praxis von den Vertretern der Vertragsparteien gefasst, die Anspruch auf einen Sitz im Ministerkomitee haben. Für diesen Beschluss ist die nach Artikel 20 Buchstabe d der Satzung des Europarats vorgesehene Zweidrittelmehrheit sowie die einhellige Zustimmung der Vertreter der Vertragsparteien erforderlich, die Anspruch auf einen Sitz im Komitee haben.

Wirkungen des Übereinkommens (Artikel 39)

307. Artikel 39 Absätze 1 und 2 behandeln das Verhältnis des Übereinkommens zu anderen völkerrechtlichen Übereinkünften oder Vereinbarungen. In den vorstehend erwähnten Musterklauseln wird die Frage, wie sich Übereinkommen des Europarats zueinander oder zu anderen außerhalb des Europarats geschlossenen zwei- oder mehrseitigen Übereinkünften verhalten sollen, nicht behandelt. In Europaratsübereinkommen auf dem Gebiet des Strafrechts (wie etwa dem Übereinkommen über den unerlaubten Verkehr auf See zur Durchführung des Artikels 17 des VN-Übereinkommens gegen den unerlaubten Verkehr mit Suchtstoffen und psychotropen Stoffen (ETS Nr. 156)) wird in der Regel Folgendes vorgesehen: (1) Neue Übereinkommen lassen die Rechte und Pflichten aus bestehenden internationalen mehrseitigen Übereinkünften über besondere Fragen unberührt; (2) Vertragsparteien eines neuen Übereinkommens können untereinander zwei- oder mehrseitige Übereinkünfte über Fragen schließen, die Gegenstand des Übereinkommens sind, um dessen Bestimmungen zu ergänzen oder zu verstärken oder um die Anwendung der darin verankerten Grundsätze zu erleichtern; und (3) haben zwei oder mehr Vertragsparteien des neuen Übereinkommens bereits ein Übereinkommen oder einen Vertrag über einen in dem neuen Übereinkommen behandelten Gegenstand geschlossen oder haben sie ihre Beziehungen in Bezug auf diesen Gegenstand auf andere Weise festgelegt, so sind sie berechtigt, anstelle des neuen Übereinkommens ein solches Übereinkommen oder einen solchen Vertrag anzuwenden oder ihre Beziehungen entsprechend zu gestalten, wenn dies die internationale Zusammenarbeit erleichtert.

308. Da das Übereinkommen im Allgemeinen zwei- oder mehrseitige Übereinkünfte und Vereinbarungen zwischen den Vertragsparteien ergänzen, nicht aber ersetzen soll, hielten die Verfasser eine möglicherweise einschränkende Bezugnahme auf „besondere Fragen“ nicht für besonders aufschlussreich und befürchteten, sie könnte zu unnötiger Unklarheit führen. Deshalb heißt es in Artikel 39 Absatz 1 nur, dass dieses Übereinkommen die zwischen den Vertragsparteien bestehenden anderen anwendbaren Übereinkünfte oder Vereinbarungen ergänzt, wobei beispielhaft u.a. insbesondere drei Übereinkommen des Europarats erwähnt werden: das Europäische Auslieferungsübereinkommen von 1957 (ETS Nr. 24), das Europäische Übereinkommen von 1959 über die Rechtshilfe in Strafsachen (ETS Nr. 30) und das Zusatzprotokoll dazu von 1978 (ETS Nr. 99). In Bezug auf allgemeine Fragen sollen die Vertragsparteien des Übereinkommens über Computerkriminalität deshalb grundsätzlich diese Übereinkünfte oder Vereinbarungen anwenden. In Bezug auf spezielle Fragen, die nur Gegenstand dieses Übereinkommens sind, gilt nach der Auslegungsregel *lex specialis derogat legi generali,* dass die Vertragsparteien vorrangig die in diesem Übereinkommen enthaltenen Regeln anwenden sollen. Ein Beispiel dafür ist Artikel 30, der die umgehende Weitergabe gesicherter Verkehrsdaten vorsieht, wenn diese zur Feststellung des Übertragungswegs einer bestimmten Kommunikation notwendig sind. Auf diesem speziellen Gebiet soll das Übereinkommen als *lex specialis* eine Regelung vorsehen, die vorrangig vor den allgemeineren Rechtshilfeübereinkünften anzuwenden ist.

309. Ebenso haben die Verfasser eine Formulierung, mit der die Anwendung bestehender oder künftiger Übereinkünfte von der Bedingung abhängig gemacht wird, dass sie die Zusammenarbeit „verstärken“ oder „erleichtern“, als möglicherweise problematisch angesehen, weil nach der Vorgehensweise im Kapitel über die internationale Zusammenarbeit davon ausgegangen wird, dass die Parteien die einschlägigen völkerrechtlichen Übereinkünfte und Vereinbarungen anwenden.

310. Soweit bereits ein Rechtshilfevertrag oder eine Vereinbarung als Grundlage für die Zusammenarbeit vorliegt, ergänzt dieses Übereinkommen, soweit erforderlich, nur die bereits bestehenden Regelungen. Dieses Übereinkommen sähe z. B. die Übermittlung von Rechtshilfeersuchen durch schnelle Kommunikationsmittel vor (siehe Artikel 25 Absatz 3), wenn diese Möglichkeit nach der ursprünglichen Übereinkunft oder Vereinbarung nicht gegeben ist.

311. Der Art des Übereinkommens als ergänzende Regelung entsprechend und insbesondere seinem Ansatz bei der internationalen Zusammenarbeit folgend ist es den Vertragsparteien nach Absatz 2 freigestellt, bereits bestehende oder in Zukunft in Kraft tretende Übereinkünfte anzuwenden. Ein Vorläufer für eine solche Formulierung findet sich in dem Übereinkommen über die Überstellung verurteilter Personen (ETS Nr. 112). Im Rahmen der internationalen Zusammenarbeit ist sicherlich zu erwarten, dass die Anwendung anderer internationaler Rechtsinstrumente (die größtenteils langjährig erprobte Formeln für die Rechtshilfe anbieten) die Zusammenarbeit tatsächlich fördern wird. Nach dem vorliegenden Übereinkommen können die Vertragsparteien auch beschließen, anstelle dieser anderen internationalen Rechtsinstrumente die Bestimmungen dieses Übereinkommens über die internationale Zusammenarbeit anzuwenden (siehe Artikel 27 Absatz 1). In diesen Fällen würden die in Artikel 27 enthaltenen einschlägigen Bestimmungen über die Zusammenarbeit die entsprechenden Vorschriften in diesen anderen internationalen Rechtsinstrumenten ersetzen. Da das vorliegende Übereinkommen im Allgemeinen Mindestverpflichtungen vorsieht, steht es den Vertragsparteien nach Artikel 39 Absatz 2 frei, über die im Übereinkommen bereits festgelegten Verpflichtungen hinaus weitere speziellere Verpflichtungen einzugehen, wenn sie ihre Beziehungen in Fragen regeln, die Gegenstand des Übereinkommens sind. Es handelt sich hierbei aber nicht um ein absolutes Recht: Die Vertragsparteien haben dabei die Zielsetzungen und Grundsätze des Übereinkommens zu achten und können daher keine Verpflichtungen übernehmen, die im Widerspruch zu seinem Zweck stehen würden.

312. Bei der Regelung des Verhältnisses zwischen dem Übereinkommen und anderen internationalen Rechtsinstrumenten waren sich die Verfasser auch dahingehend einig, dass die Vertragsparteien sich ferner von den einschlägigen Bestimmungen des Wiener Übereinkommens über das Recht der völkerrechtlichen Verträge leiten lassen können.

313. Obwohl das Übereinkommen einen dringend benötigten Grad an Harmonisierung herstellt, nimmt es nicht für sich in Anspruch, alle noch offenen Fragen im Zusammenhang mit der Computerkriminalität zu behandeln. Deshalb wurde Absatz 3 eingefügt, um klarzustellen, dass das Übereinkommen nur das berührt, was darin

behandelt wird. Unberührt bleiben andere Rechte, Beschränkungen, Pflichten und Verantwortlichkeiten, die gegebenenfalls bestehen, in dem Übereinkommen aber nicht behandelt werden. Vorläufer für eine solche „einschränkende Klausel" finden sich in anderen völkerrechtlichen Übereinkünften (wie dem Übereinkommen der Vereinten Nationen zur Bekämpfung der Terrorismus-Finanzierung).

Erklärungen (Artikel 40)

314. In Artikel 40 wird auf einige Artikel verwiesen, die hauptsächlich die Straftaten betreffen, die nach dem Übereinkommen im Abschnitt über das materielle Recht festzulegen sind, und bei denen die Vertragsparteien einige bestimmte zusätzliche Merkmale aufnehmen können, die den Anwendungsbereich der Bestimmungen verändern. Mit diesen zusätzlichen Merkmalen soll bestimmten begrifflichen und rechtlichen Unterschieden Rechnung getragen werden, die in einer Übereinkunft mit globaler Zielsetzung eher vertretbar sind als möglicherweise in einem rein europaratsbezogenen Zusammenhang. Als Erklärungen gelten hinnehmbare Auslegungen der Bestimmungen eines Übereinkommens; sie sind zu unterscheiden von Vorbehalten, mit denen eine Vertragspartei die rechtliche Wirkung bestimmter im Übereinkommen enthaltener Verpflichtungen ausschließen oder verändern kann. Da es für die Vertragsparteien des Übereinkommens wichtig ist zu wissen, ob und gegebenenfalls welche zusätzlichen Merkmale von anderen Vertragsparteien hinzugefügt wurden, muss dem Generalsekretär des Europarats gegenüber bei der Unterzeichnung oder bei der Hinterlegung einer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde eine Erklärung dazu abgegeben werden. Diese Notifikation ist besonders bei der Definition von Straftaten wichtig, denn das Erfordernis der beiderseitigen Strafbarkeit muss bei den Vertragsparteien erfüllt sein, wenn sie bestimmte verfahrensrechtliche Befugnisse ausüben. Eine Begrenzung der Zahl der Erklärungen wurde nicht für nötig erachtet.

Bundesstaatsklausel (Artikel 41)

315. Damit der Zielvorgabe entsprechend möglichst viele Staaten Vertragsparteien des Übereinkommens werden können, ist nach Artikel 41 ein Vorbehalt zulässig, mit dem den Schwierigkeiten Rechnung getragen werden kann, denen sich Bundesstaaten aufgrund ihrer charakteristischen Gewaltverteilung zwischen Zentral- und Regionalbehörden gegenübersehen können. Außerhalb des strafrechtlichen Bereichs gibt es Vorläufer für solche föderalen Erklärungen oder Vorbehalte zu anderen völkerrechtlichen Übereinkünften[11]). Hier wird durch Artikel 41 anerkannt, dass aufgrund der bestehenden innerstaatlichen Gesetzgebung und Praxis einer Vertragspartei, die ein Bundesstaat ist, geringfügige Abweichungen bei der Anwendung auftreten können. Diese Abweichungen müssen durch die Verfassung des Bundesstaates oder durch andere Grundprinzipien der Gewaltverteilung in Angelegenheiten der Strafrechtspflege zwischen der Zentralregierung und den Gliedstaaten oder Gebietseinheiten eines Bundesstaates begründet sein. Die Verfasser des Übereinkommens waren sich einig, dass die Anwendung der Bundesstaatsklausel nur zu geringfügigen Abweichungen bei der Durchführung des Übereinkommens führen wird.

316. In den Vereinigten Staaten von Amerika z. B. ist nach der Verfassung und den Grundprinzipien des Föderalismus vorgesehen, dass die Bundesstrafgesetze im Allgemeinen Tatbestände insoweit regeln, als sie sich auf den Handel zwischen den Gliedstaaten oder mit dem Ausland auswirken, wohingegen Sachen mit geringer oder rein lokaler Tragweite traditionell von den Gliedstaaten geregelt werden. Nach dieser Sichtweise des Föderalismus fallen die von diesem Übereinkommen erfassten rechtswidrigen Handlungen zwar weitgehend unter das amerikanische Bundesstrafrecht, doch es wird anerkannt, dass die Gliedstaaten weiterhin für Handlungen zuständig sind, die nur geringfügige Auswirkungen oder rein lokalen Bezug haben. In einigen Fällen kann es vorkommen, dass ein Gliedstaat in dieser eng gefassten Kategorie von Handlungen, die durch einzelstaatliches Recht und nicht durch Bundesrecht geregelt sind, eine Maßnahme nicht vorsieht, die ansonsten unter das Übereinkommen fallen würde. So kann z. B. ein Angriff auf einen Einzelplatz-PC oder auf ein Netz von Computern, die in einem einzelnen Gebäude untereinander verbunden sind, nur dann strafbar sein, wenn dies nach dem Recht des Staates, in dem der Angriff stattgefunden hat, vorgesehen ist; der Angriff wäre jedoch eine Straftat nach Bundesrecht, wenn der Zugriff auf den Computer über das Internet erfolgt, denn die Nutzung des Internets stellt die für die Heranziehung des Bundesrechts nötige Auswirkung auf den Handel zwischen den Gliedstaaten oder mit dem Ausland dar. Die Durchführung dieses Übereinkommens durch das Bundesrecht der Vereinigten Staaten oder durch das Recht eines anderen Bundesstaats unter ähnlichen Bedingungen würde den Voraussetzungen nach Artikel 41 entsprechen.

317. Der Geltungsbereich der Bundesstaatsklausel ist auf Kapitel II beschränkt worden (materielles Strafrecht, Verfahrensrecht und Gerichtsbarkeit). Bundesstaaten, die von dieser Bestimmung Gebrauch machen, wären weiterhin zur Zusammenarbeit mit den anderen Vertragsparteien nach Kapitel III auch dann verpflichtet, wenn der Gliedstaat oder eine andere gleichartige Gebietseinheit, in der sich ein Verfolgter oder Beweismaterial befindet, die Handlung nicht mit Strafe bedroht oder nicht über die nach dem Übereinkommen vorgeschriebenen Verfahren verfügt.

318. Nach Artikel 41 Absatz 2 kommt hinzu, dass ein Bundesstaat, der einen Vorbehalt nach Absatz 1 anbringt, diesen Vorbehalt nicht anwenden darf, um seine Verpflichtungen nach Kapitel II auszuschließen oder wesentlich einzuschränken. Er hat auf jeden Fall umfassende und wirksame Strafverfolgungsmöglichkeiten in Bezug auf Maßnahmen nach Kapitel II vorzusehen. Bestimmungen, deren Durchführung in die gesetzgeberische Zuständigkeit der Gliedstaaten oder anderer gleichartiger Gebietseinheiten fällt, leitet die Bundesregierung an die Behörden dieser Einheiten mit einer befürwortenden Stellungnahme weiter und ermutigt sie, geeignete Maßnahmen zu treffen, um diese Bestimmungen wirksam werden zu lassen.

Vorbehalte (Artikel 42)

319. Artikel 42 sieht eine Reihe möglicher Vorbehalte vor. Diese Vorgehensweise ist darauf zurückzuführen, dass das Übereinkommen einen Bereich des Strafrechts und des Strafverfahrensrechts behandelt, der für viele Staaten relativ neu ist. Außerdem erfordert die Globalität

des Übereinkommens, das für Mitglied- und Nichtmitgliedstaaten des Europarats offen stehen wird, solche Vorbehaltsmöglichkeiten. Mit diesen Vorbehaltsmöglichkeiten sollen möglichst viele Staaten Vertragsparteien des Übereinkommens werden und dabei gleichzeitig bestimmte ihrem innerstaatlichen Recht entsprechende Vorgehensweisen und Konzepte beibehalten können. Gleichzeitig haben sich die Verfasser bemüht, die Möglichkeiten der Anbringung eines Vorbehalts zu beschränken, um eine möglichst einheitliche Anwendung des Übereinkommens durch die Vertragsparteien sicherzustellen. So dürfen keine anderen als die aufgeführten Vorbehalte angebracht werden. Außerdem darf eine Vertragspartei Vorbehalte nur bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde anbringen.

320. In der Erkenntnis, dass für einige Vertragsparteien bestimmte Vorbehalte zur Vermeidung von Konflikten mit ihren Verfassungsgrundsätzen oder rechtlichen Grundprinzipien unbedingt nötig waren, wurde in Artikel 43 keine spezielle Frist für die Rücknahme von Vorbehalten festgelegt. Vielmehr sollen sie zurückgenommen werden, sobald die Umstände dies erlauben.

321. Um einen gewissen Druck auf die Vertragsparteien auszuüben und um sie zu veranlassen, die Rücknahme ihrer Vorbehalte zumindest zu prüfen, ist der Generalsekretär des Europarats nach dem Übereinkommen befugt, sich in regelmäßigen Abständen nach den Aussichten für eine Rücknahme zu erkundigen. Diese Möglichkeit der Nachfrage ist gängige Praxis im Rahmen mehrerer Europaratsübereinkommen. Den Vertragsparteien wird damit Gelegenheit gegeben, mitzuteilen, ob sie ihre Vorbehalte zu bestimmten Vorschriften aufrechterhalten müssen, und anschließend diejenigen zurückzunehmen, die sich als nicht mehr notwendig erweisen. Die Vertragsparteien werden hoffentlich im Laufe der Zeit in der Lage sein, möglichst viele Vorbehalte zurückzunehmen, so dass die einheitliche Anwendung des Übereinkommens gefördert wird.

Änderungen (Artikel 44)

322. Artikel 44 geht auf eine vergleichbare Bestimmung im Übereinkommen über Geldwäsche sowie Ermittlung, Beschlagnahme und Einziehung von Erträgen aus Straftaten (ETS Nr. 141) zurück, wo sie als Neuerung in Bezug auf Strafrechtsübereinkommen eingeführt wurde, die im Rahmen des Europarats ausgearbeitet werden. Das Änderungsverfahren ist hauptsächlich für vergleichsweise kleine Änderungen prozessualer und technischer Natur gedacht. Die Verfasser waren der Ansicht, dass bedeutendere Änderungen des Übereinkommens in Form von Zusatzprotokollen erfolgen könnten.

323. Die Vertragsparteien können nach dem Konsultationsverfahren nach Artikel 46 selbst prüfen, ob Änderungen oder Protokolle nötig sind. Der Lenkungsausschuss für Strafrechtsfragen (CDPC) wird regelmäßig hiervon unterrichtet und soll die erforderlichen Maßnahmen treffen, um die Vertragsparteien bei ihren Bemühungen um Änderung oder Ergänzung des Übereinkommens zu unterstützen.

324. Nach Absatz 5 tritt eine beschlossene Änderung erst in Kraft, wenn alle Vertragsparteien dem Generalsekretär mitgeteilt haben, dass sie sie angenommen haben. Mit diesem Erfordernis soll sichergestellt werden, dass das Übereinkommen sich einheitlich weiterentwickelt.

Beilegung von Streitigkeiten (Artikel 45)

325. In Artikel 45 Absatz 1 heißt es, dass der Lenkungsausschuss für Strafrechtsfragen (CDPC) über die Auslegung und Anwendung der Bestimmungen des Übereinkommens auf dem Laufenden zu halten ist. Absatz 2 verpflichtet die Vertragsparteien, sich um eine friedliche Beilegung von Streitigkeiten über die Auslegung oder Anwendung des Übereinkommens zu bemühen. Jedes Verfahren zur Streitbeilegung soll von den betroffenen Vertragsparteien vereinbart werden. Die Bestimmung schlägt drei mögliche Mechanismen zur Streitbeilegung vor: den Lenkungsausschuss für Strafrechtsfragen (CDPC) selbst, ein Schiedsgericht oder den Internationalen Gerichtshof.

Konsultationen der Vertragsparteien (Artikel 46)

326. Artikel 46 schafft einen Rahmen für die Vertragsparteien zur Konsultation über die Durchführung des Übereinkommens, die Folgen wichtiger rechtlicher, politischer oder technischer Entwicklungen in Bezug auf die Computerkriminalität und die Erhebung von Beweisen in elektronischer Form sowie die Möglichkeit einer Ergänzung oder Änderung des Übereinkommens. Gegenstand der Konsultationen werden insbesondere Fragen sein, die sich bei der Nutzung und Durchführung des Übereinkommens ergeben haben, einschließlich der Wirkungen von Erklärungen und Vorbehalten nach den Artikeln 40 und 42.

327. Das Verfahren ist flexibel, und es bleibt den Vertragsparteien überlassen zu entscheiden, wie und wann sie zusammentreten, falls sie dies wünschen. Die Verfasser des Übereinkommens haben dieses Verfahren für erforderlich erachtet, um sicherzustellen, dass gegebenenfalls alle Vertragsparteien des Übereinkommens einschließlich der Nichtmitgliedstaaten des Europarats gleichberechtigt an einem Mechanismus für Folgemaßnahmen beteiligt werden können und gleichzeitig die Zuständigkeiten des Lenkungsausschusses für Strafrechtsfragen (CDPC) erhalten bleiben. Der CDPC ist nicht nur regelmäßig über die Konsultationen zwischen den Vertragsparteien zu unterrichten, sondern hat diese auch zu fördern und die erforderlichen Maßnahmen zu treffen, um die Vertragsparteien bei ihren Bemühungen um Ergänzung oder Änderung des Übereinkommens zu unterstützen. In Anbetracht der Erfordernisse einer wirksamen Verhütung und Verfolgung der Computerkriminalität sowie der damit verbundenen Datenschutzfragen, der möglichen Auswirkungen auf den Geschäftsverkehr und anderer einschlägiger Faktoren können die Ansichten interessierter Stellen einschließlich Strafverfolgungsbehörden sowie nichtstaatlicher und privatwirtschaftlicher Organisationen für diese Konsultationen hilfreich sein (siehe auch Nr. 14).

328. In Absatz 3 ist vorgesehen, dass die Durchführung des Übereinkommens drei Jahre nach seinem Inkrafttreten überprüft wird; zu diesem Zeitpunkt können geeignete Änderungen empfohlen werden. Der CDPC führt diese Überprüfung mit Unterstützung der Vertragsparteien durch.

329. In Absatz 4 heißt es, dass die Vertragsparteien Konsultationen nach Artikel 46 Absatz 1 selbst finanzieren, soweit die Kosten nicht vom Europarat übernommen werden. Neben dem Lenkungsausschuss für Strafrechtsfragen (CDPC) wird jedoch auch das Sekretariat des Europarats die Vertragsparteien bei ihren Bemühungen im Zusammenhang mit dem Übereinkommen unterstützen.

Fußnoten:

[1]) Durchführung der Empfehlung Nr. R (89) 9 über computerbezogene Straftaten. Bericht von Prof. H.W.K. Kaspersen (Dok. CDPC (97) 5 und PC-CY (97) 5, S. 106).

[2]) Siehe Computerkriminalität, Bericht des Lenkungsausschusses für Strafrechtsfragen, S. 86.

[3]) Siehe strafverfahrensrechtliche Probleme im Zusammenhang mit der Informationstechnologie, Empfehlung Nr. R (95) 13, Grundsatz Nr. 17.

[4]) Der Wortlaut der Konvention war in Übereinstimmung mit dem Protokoll Nr. 3 (ETS Nr. 45), das am 21. September 1970 in Kraft getreten ist, dem Protokoll Nr. 5 (ETS Nr. 55), das am 20. Dezember 1971 in Kraft getreten ist, und dem Protokoll Nr. 8 (ETS Nr. 118), das am 1. Januar 1990 in Kraft getreten ist, geändert worden und enthielt auch den Wortlaut des Protokolls Nr. 2 (EZS Nr. 44), das gemäß Artikel 5 Absatz 3 dieses Protokolls seit seinem Inkrafttreten am 21. September 1970 Bestandteil der Konvention war. Alle mit diesen Protokollen geänderten oder ergänzten Bestimmungen wurden durch das Protokoll Nr. 11 (ETS Nr. 155) ab dessen Inkrafttreten am 1. November 1998 ersetzt. Mit diesem Datum wurde das am 1. Oktober 1994 in Kraft getretene Protokoll Nr. 9 (ETS Nr. 140) aufgehoben und wurde das Protokoll Nr. 10 (ETS Nr. 146) gegenstandslos.

[5]) EGMR-Urteil in der Sache Klass ./. Deutschland, A28, 06/09/1978

[6]) EGMR-Urteil in der Sache Kruslin ./. Frankreich, 176-A, 24/04/1990

[7]) EGMR-Urteil in der Sache Huvig ./. Frankreich, 176-B, 24/04/1990

[8]) EGMR-Urteil in der Sache Malone ./. Vereinigtes Königreich, A82, 02/08/1984

[9]) EGMR-Urteil in der Sache Halford ./. Vereinigtes Königreich, Berichte 1997 – III, 25/06/1997

[10]) EGMR-Urteil in der Sache Lambert ./. Frankreich, Berichte 1998 – V, 24/08/1998

[11]) Beispielsweise das Abkommen vom 28. Juli 1951 über die Rechtsstellung der Flüchtlinge, Artikel 34; das Übereinkommen vom 28. September 1954 über die Rechtsstellung der Staatenlosen, Artikel 37; das Übereinkommen vom 10. Juni 1958 über die Anerkennung und Vollstreckung ausländischer Schiedssprüche, Artikel 11; das Übereinkommen vom 16. November 1972 zum Schutz des Kultur- und Naturerbes der Welt, Artikel 34.

Anlage 2

Stellungnahme des Nationalen Normenkontrollrates

Der Nationale Normenkontrollrat hat den Entwurf des Gesetzes auf Bürokratiekosten, die durch Informationspflichten begründet werden, geprüft.

Mit dem Gesetz werden zwei neue Informationspflichten für die Verwaltung eingeführt. Informationspflichten der Wirtschaft und für Bürgerinnen und Bürger sind durch das Gesetz nicht betroffen.

Der Nationale Normenkontrollrat hat im Rahmen seines gesetzlichen Prüfauftrages keine Bedenken gegen das Regelungsvorhaben. Sollten sich in der weiteren Abstimmung des Regelungsentwurfs Änderungen ergeben, die Informationspflichten betreffen, bitten wir um erneute Beteiligung.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333